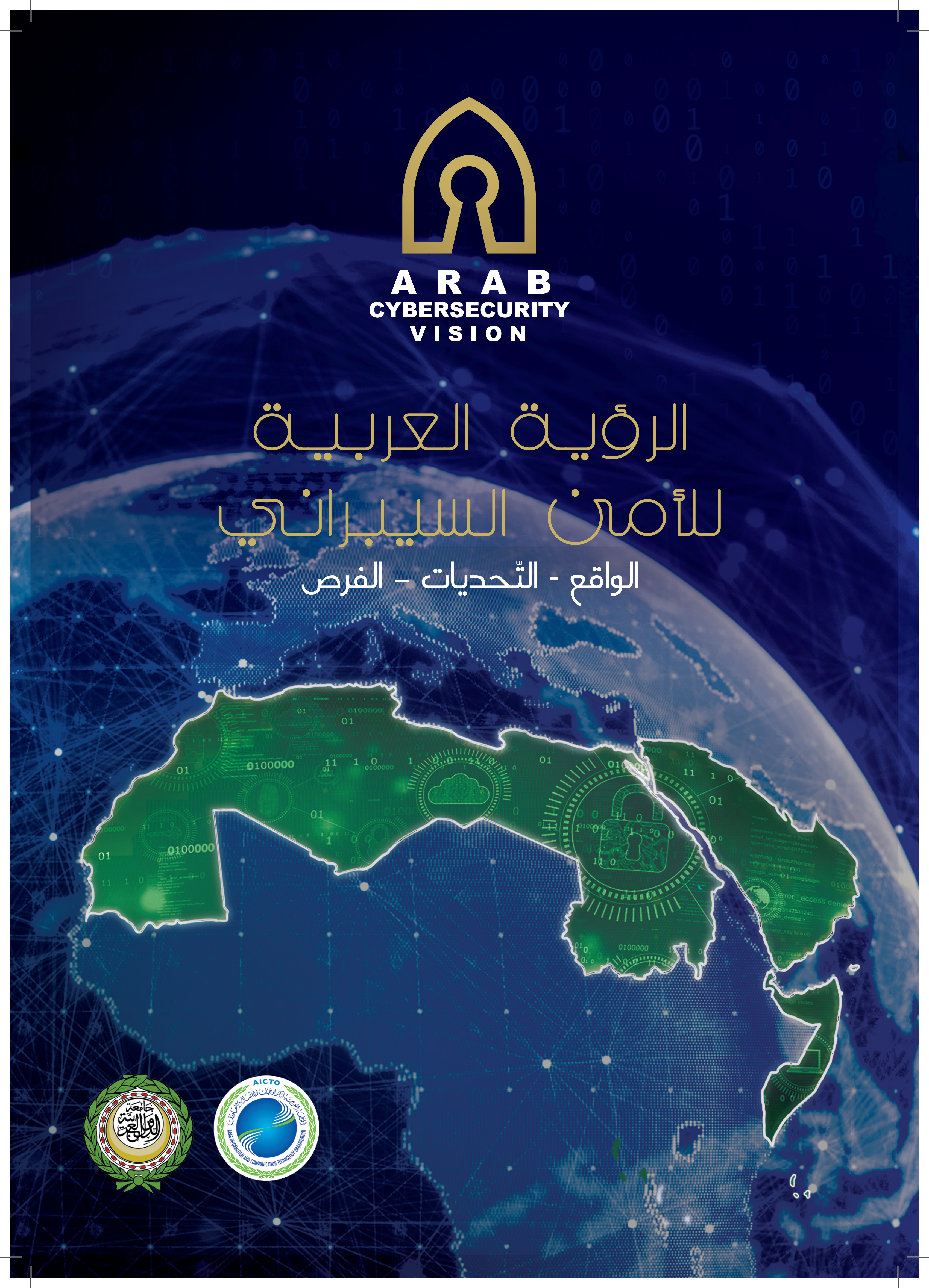
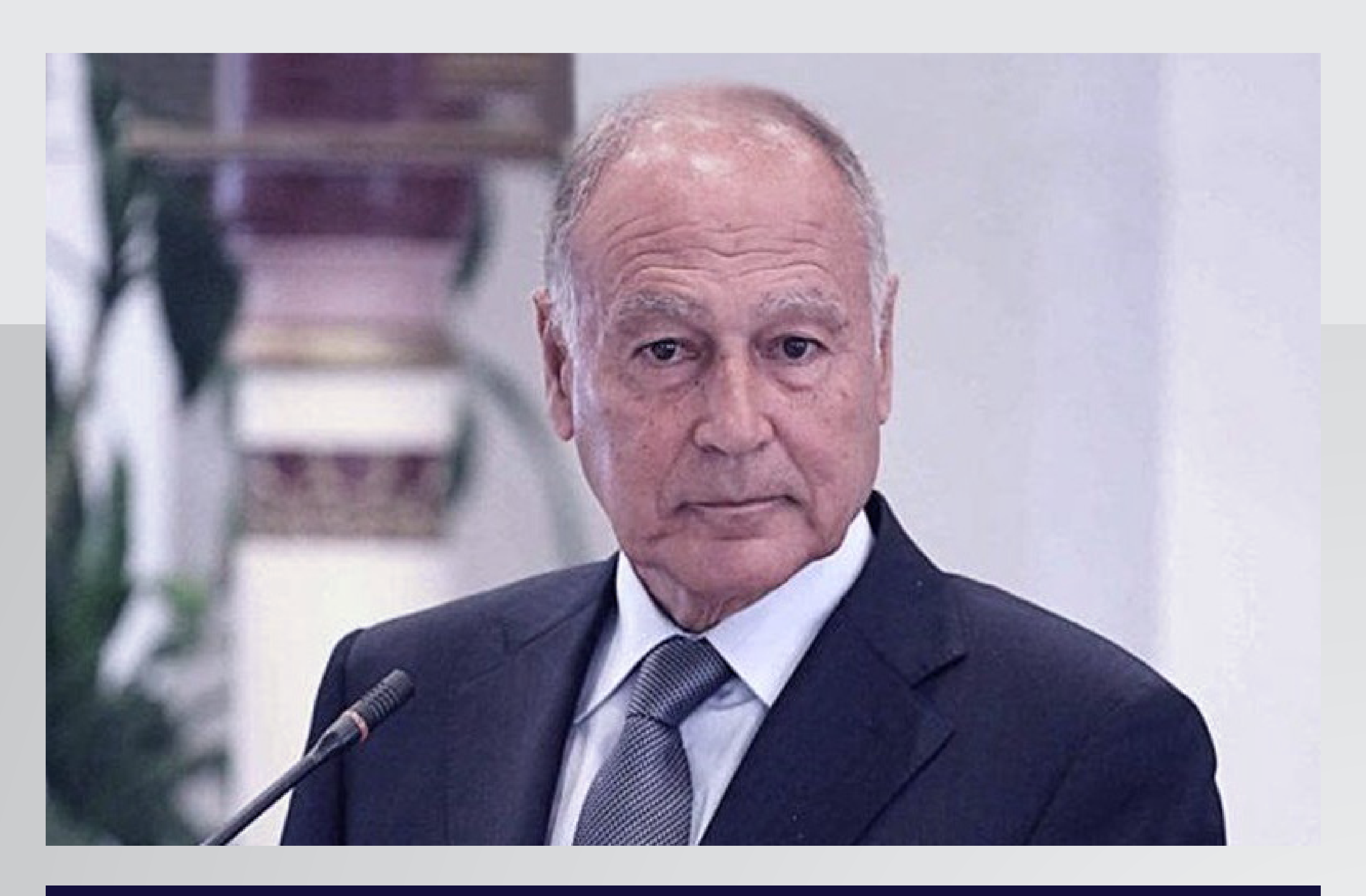

ARAB
CYBERSECURITY
VISION
الرؤية العربية
للأمن السيبراني
الواقع - التّحديات - الفرص
AICTO





الأمين العام لجامعة الدول العربية

لقد شهد موضوع أمن البيانات مؤخراً تطورات هامة على الصعيد الدولي... حيث شكلت الأمم المتحدة لجنة مفتوحة العضوية لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام التكنولوجيا لأغراض إجرامية... وهي لجنة ستبدأ عملها قريباً... وعلينا كعرب أن نشارك بفاعلية في أعمالها لحماية حقوقنا والدفاع عنها

وفي ذات السياق، كنا قد شكلنا في الدورة السابقة للجنة التنسيق العليا فريق عمل لوضع إطار عربي موحد لمواجهة القرصنة الالكترونية وحماية الشبكات. .كما دعونا .. إلى تنظيم منتدى عربي لمناقشة تحديات الأمن السيبراني. . والذي أتطلع إلى إقامته في أقرب فرصة ممكنة وأتمنى أن تشارك فيه كافة الدول الأعضاء ومؤسسات العمل العربي المشترك بشكل فاعل.

مقتطف من كلمة السيد أحمد أبو الغيط
الأمين العام لجامعة الدول العربية
خلل افتتاح أعمال الدورة (51)
للجنة التنسيق العليا للعمل العربي المشترك - مدينة العلمين الجديدة : 2021/7/8



رئيس المجلس التنفيذي للمنظمة

شهد العالم في السنوات الماضية الكثير من التطورات المتسارعة في الفضاء السيبراني، وما زلنا نشهد رقمنة مختلف جوانب الحياة والخدمات وابتكار تكنولوجيات جديدة، ومع كل مرحلة تطورية في قطاع الاتصالات وتكنولوجيا المعلومات نشهد كذلك ظهور تحديات جديدة.
ان قضية الامن السيبراني اصبحت موضع اهتمام بشكل متزايد خلال الفترة الماضية لاسيما بعد جائحة
كوفيد-١٩ التي اضطرت العديد من القطاعات الى الاعتماد على تكنولوجيا المعلومات والاتصالات بشكل اكبر من ذي قبل، وبدأت تظهر العديد من الابعاد في هذا السياق، معظمها ذات طبيعة عابرة للحدود الجغرافية للدول، كالاخبار المزيفة واخلاقيات الفضاء السيبراني والدبلوماسية السيبرانية والسيادة الرقمية، دلالة على تنامي التحديات والتهديدات في هذا المجال.
اود ان اغتنم هذه الفرصة كي نعلن عن اطلاق النسخة الاولى من الرؤية العربية للامن السيبراني، التي تقدم حصيلة لأهم ما توصل اليه فريق الخبراء المكلف بوضع هذه الرؤية متضمنا الوضع الحالي في الدول العربية ونماذج المخاطر السيبرانية التي تواجهها كما تقدم مقترحا لرؤية استراتيجية عربية مشتركة للأمن السيبرني وأخيرا مقترحات حول مسألة حوكمة الامن السيبراني في المنطقة العربية وبعض المبادرات التي يمكن تنفيذها. آملين ان تنال رضا واستحسان الدول العربية وتساهم في تعزيز قطاع الامن السيبراني لديها.

سعادة السيد أمير البياتي
رئيس المجلس التنفيذي للمنظمة



المدير العام للمنظمة العربية لتكنولوجيات الاتصال و المعلومات

يعيش العالم منذ سنوات على وقع الثورة الرقميّة، التي تعرف بالثورة الصناعية الرابعة والتي فتحت الباب على مصراعيه للإمكانيات اللامحدودة للوصول إلى المعرفة وتوفير الخدمات من خلال العديد من التوجّهات التكنولوجية التي تتطوّر يوما بعد يوم كـ : الذكاء الاصطناعي، والروبوتات، وإنترنت الأشياء، المركبات ذاتية القيادة، الطباعة ثلاثية الأبعاد، وتكنولوجيا النانو، التكنولوجيا الحيوية، تكنولوجيا الملاحة بالأقمار الصناعية، سلسلة الكتل (Blockchain)، وغيرها.

ومع بداية سنة 2020 وإنتشار جائحة كورونا على المستوى العالمي، تعزز الدور الريادي الذي تلعبه التكنولوجيا في حياتنا وأصبحت العامل الحيوي، الوحيد تقريبا، لفك العزلة عن الأشخاص ومواصلة العديد من القطاعات الاقتصادية : كالتعليم والشغل والمواصلات والصحة وغيرها، .... وبالتالي، أصبح التحول إلى الحلول الرقميّة على جميع الأصعدة ضروريا وليس خيارا للتعامل مع هذه الأزمة الصحية والحد من آثارها السلبية.

ولم تكن بلداننا العربية بمنأى عن هذه التطوّرات والمتغيّرات العالمية، فكانت مجبرة على فرض تدابير وقائية، صارمة في بعض الأحيان، واضطرت جل الدول العربية إلى تسخير كل إمكانياتها في سبيل الحد من إنتشار الأزمة. وقد شاهدنا إنتقالا كبيرا إلى الخدمات والحلول الرقمية في العديد من الدول، سواء الجاهزة منها أو غير الجاهزة، الشيء الذي ضاعف التهديدات والمخاطر السيبرانية.

(Volatile, Uncertain, Complex and Ambiguous) VUCA World.

اليوم، وبعد تجربتنا مع جائحة كورونا، علينا الإقرار أننا أصبحنا نعيش في عالم سريع التغيير يمكن وصفه بـ : المتقلب، غير المؤكد، معقد وغامض، وهو ما يعبر عنه باللغة الإنجليزية بـ

في هذا العالم لم تعد القواعد القديمة سارية المفعول. وحتى لا نتخلف على الركب، يتعين على الدول العربية أن تكون قادرة على التنبؤ بالمستقبل والتكيف مع المتغيّرات بنفس الوتيرة، مع التحلي بالمرونة لا سيما في رسم السياسات وتنفيذها، لا سيما في القطاع التكنولوجي والرقمي.

وهنا لا يمكننا التطرّق إلى مسألة الاقتصاد الرقمي أو المرور إلى المجتمعات الرقمية، دون الإشارة أن موضوع الأمن السيبراني هو من أهم المقومات الرئيسية والداعمة لنجاح بناء إقتصاد رقمي قوي داخل أي دولة.

وفي هذا الإطار، ومن منطلق وعيها بأن التعامل مع المخاطر السيبرنية التي تتزايد يوما بعد يوم، يطلّب توحيد الجهود على المستوى العربي والاقليمي لإيجاد حلول شاملة تخدم الجميع، بادرت المنظمة العربية لتكنولوجيات الاتصال والمعلومات، إستنادا إلى قرار القمة العربية التنموية عدد56 بتاريخ 20 جانفي 2019 بالعمل صياغة "الرؤية العربية الموحدة للأمن السيبراني"، في إطار مساهمتنا في تعزيز العمل العربي المشترك ومساعدة الدول العربية على العمل في إطار تكاملي وتشاركي بشكل يضمن الازدهار والرقي لبلداننا العربية في المجال الرقمي.

الشكر موصول لجامعة الدول العربية على دعمها لنا في هذه المبادرة ونتمنى أن تكون هذه "الرؤية العربية الموحدة للأمن السيبراني"، نقطة بداية لخط إستراتيجيات ومبادرات عربية مشتركة في مجال الأمن السيبراني، خاصّة وأن المنطقة لديها الكثير من الطاقات البشرية في هذا المجال وكذلك التجارب الناجحة على المستوى العالمي.

"لنعمل معا من أجل مجتمع رقمي عربي آمن"

المهندس / محمد بن عمر

المدير العام للمنظمة العربية لتكنولوجيات الاتصال والمعلومات



وزير تكنولوجيات الاتصال التونسي

"الإستراتيجية الوطنية للأمن السيبرني تشمل الإجراءات والتدابير التقنية وغير التقنية. أمّا فيما يتعلق بالتدابير التقنية فهي بالأساس:

- الإجراءات الاستباقية لتفادي التهديدات المحتملة على الفضاء السيبرني سواء كانت عرضية أو متعمدة وذلك بتحليل بيانات شبكات الاتصال وأنظمة المعلومات وإدراج حلول الذكاء الاصطناعي.
- إجراءات التوقي التي ترتكز بالأساس على التدقيق الدوري في سلامة الشبكات وأنظمة المعلومات لكشف وإصلاح الثغرات.
- إجراءات التفطن المبكر للحوادث والهجمات السيبرنية باعتماد أنظمة المراقبة والمنصات المخصصة للإبلاغ عن الهجمات المحتملة.
- الإجراءات الاستعجالية لتامين الاستجابة الناجعة في حالات الطوارئ للتصدي السريع للهجمات والحد من التداعيات المحتملة على النظم والشبكات.
- إجراءات التعافي السريع لضمان استمرارية النشاط ومجابهة الكوارث المحتملة.
- إجراءات التحقيق والتحري الرقمي لجمع الأدلة وتشخيص الحوادث السيبرنية ورصد مصادر الخطر وتحديد المسؤوليات واستخلاص الدروس لتحسين التدابير التي سبق ذكرها بصفة مستمرة.

أمّا فيما يتعلق بالإجراءات الغير تقنية فهي كالأتي:

- مراجعة واستكمال النصوص التشريعية والقانونية التي تعنى بالسلامة المعلوماتية والجرائم الالكترونية.
- تعزيز وتدعيم الهياكل المسؤولة على تامين الفضاء السيبرني.
- تأهيل الكفاءات الوطنية وتطوير المهارات في مجال السلامة المعلوماتية.
- تعزيز اليقظة التكنولوجية والتشجيع على البحث العلمي والتجديد في مجال السلامة المعلوماتية.
- الانضمام إلى المعاهدات والمنظمات الدولية الناشطة في مجال السلامة المعلوماتية وإبرام اتفاقيات وعقد شراكات دولية في هذا المجال باعتبار أن الفضاء السيبرني فضاء مشترك ومفتوح.
- وضع سياسة اتصال وتواصل ناجعة لتحسيس العموم وضمان التنسيق مع مختلف الأطراف الفاعلة في مجال الأمن السيبرني.

مقتطف من كلمة الدكتور نزار بن ناجي

وزير تكنولوجيات الاتصال التونسي بمناسبة المنتدى العربي للأمن السيبرني

جدول المحتويات

ملخص تنفيذي

في ظل التصاعد السريع لمفهوم القدرات السيبرانية والذي يعد وبشكل رسمي احد ادوات الحروب الحديثة بل واصبح يمثل احد القطاعات الرئيسية في الكثير من جيوش الدول المتقدمة فيما يطلق عليه "العمليات السيبرانية الهجومية" وبعد عشرات من النماذج الموثقة والمعلنة حول اختراقات اثرت على تقويض قدرات دول كبرى بهجمات الكترونية اثرت احيانا علي بنيتها التحتية الحرجة او مصادر الطاقة بها ومرورا بانتهاك سرية بيانات العديد من المؤسسات والحكومات في كل انحاء العالم وانتهاء بالتاثير علي نتاج الانتخابات عن طريق هجمات الكترونية كما حدث في الانتخابات الامريكية ما قبل الاخيرة.
بات جديرا بالدول العربية ان تمتلك الادوات والتقنيات المناسبة بالاضافة الي المناخ التشريعي الملائم والكافي من اجل حماية الاصول الرقمية للدول العربية وحماية امن بيانات وخصوصية مواطنيها حيث اصبح الامن السيبراني قضية امن قومي في المقام الاول ولم يعد بحالة من الاحوال امرا تقنيا او نوعا من الرفاهية .
وعلى الرغم من ان الجهد المبذول خلال السنوات الأخيرة من بعض الدول العربية في بناء قدراتها السيبرانية كان له الأثر المميز في وضعها ضمن مصاف الدوا المتقدمة في العديد من المؤشرات الدولية المتخصصة الا ان نسبة ليست بالقليلة ما ذالت في مراحل مبكرة في هذا الشان.
من هذا المنطلق سعت المنظمة العربية لتكنولوجيا المعلومات والاتصالات لطرح هذه الرؤية من اجل القاء الضوء على الفرص والتحديات المحيطة بأمن الفضاء السيبراني العربي من اجل تحفيز اهمية التعاون العربي المشترك في هذا الصدد وتقديم رؤية تسعى لدعم التكامل العربي نحو فضاء عربي آمن يحقق الرخاء لشعوب المنطقة العربية ويدعم اندماج الاقتصاد الرقمي العربي في الاقتصاد الرقمي العالمي محققا النماء والتكامل والرفاهية لشعوب المنطقة.
وتقدم هذه الوثيقة حصيلة لأهم ما توصل اليه فريق الخبراء المكلف بوضع هذه الرؤية متضمنا الوضع الحالي في الدول العربية ونماذج المخاطر السيبرانية التي تواجها كما تقدم هذه الوثيقة مقترحا لرؤية استراتيجية عربية مشتركة للأمن السيبرني وأخيرا مقترحات حول مسألة حوكمة الامن السيبراني في المنطقة العربية وبعض المبادرات التي يمكن تنفيذها.



١.

الباب الأول

إطار الدراسة

1.1 مؤشرات عامة

شهدت المعطيات الديموغرافية في المنطقة العربية تطورا هاما خلال العقود الأخيرة. حيث يبلغ عدد السكان اليوم حوالي 423 مليون نسمة، مقارنة ب222,7 مليونا سنة 1990. ويمثل عدد سكان المنطقة العربية اليوم 5,6 بالمائة من سكان العالم يتوزعون على 22 دولة تغطي عشر مساحة اليابسة (14 مليون كلم.). وتتميز المنطقة العربية بنسبة شباب عالية إذ تشكل الفئة العمرية 10-24 سنة زهاء ربع إجمالي سكان المنطقة.

وبالرجوع إلى المؤشرات الدولية، يبدو واضحا أن مستويات التنمية الاقتصادية والاجتماعية والبشرية غير متوازنة بين الدول العربية. حيث يرتقي ترتيب بعض الدول إلى مستوى يقترب من كوكبة الدول المتقدمة بينما تجابه دول أخرى صعوبات مع التنمية نظرا للمتغيرات الاقتصادية الأساسية والبنية الاجتماعية والاقتصادية والصراعات وغيرها من المعوقات التي تمس المنطقة ومحيطها. وكان لموجة كوفيد-19، الازمة الصحية الأكبر التي يواجها العالم بأسره، الأثر في تعميق هذا الاختلال في التوازن خاصة وأن بعض الدول كانت جاهزة لتوظيف حلول رقمية قصد استيعاب التغيرات العميقة في أساليب العمل والإنتاج وتقديم الخدمات عن بعد في حين لم تكن دول أخرى قادرة على تحقيق الانتقال السلس والمرن من الخدمات الحضورية الى الخدمات عن بعد.

ويرجع تفاقم الهوة بين دول المنطقة إلى تباين تطور البنى التحتية والكفاءات ومنظومات البحث والتطوير والأنظمة التشريعية.

في خضم التطورات الرقمية المتسارعة التي يشهدها الاقتصاد العالمي، بدأت دول المنطقة العربية في التحول من الاقتصاد التقليدي إلى الاقتصاد الرقمي. وقد أحرزت بعض الدول تقدما ملحوظا في رقمنة عدد من المجالات والقطاعات المختلفة. كما بينت دراسة نشرها صندوق النقد العربي سنة 2020 أن الاقتصاد الرقمي ساهم على سبيل المثال في خفض تكلفة إنجاز الخدمات الحكومية بنسبة تصل إلى 88 في المائة في بعض الدول بينما لا تزال دول أخرى تنخرط ببطء شديد في التحولات الرقمية. ومن المتوقع أن يكون للهوة الرقمية دور في توسيع الفجوة الاقتصادية بين بلدان المنطقة.

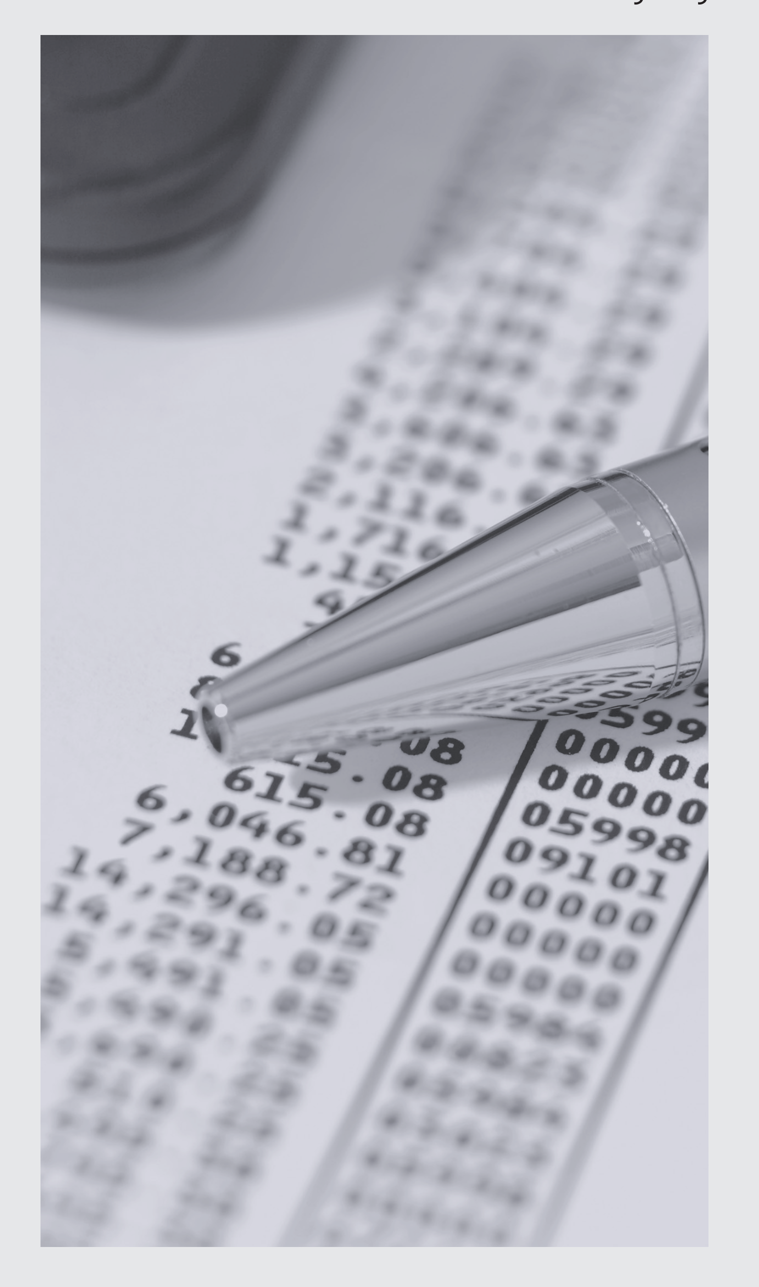
في ضوء ما سبق، يتنزل الأمن السيبراني ضمن الأولويات الاستراتيجية في دول المنطقة العربية. حيث أن انفتاح الفضاءات السيبرانية على محيطها ما فتئ أمرا حتميا يفتح تحديات جمة ناهيك أن الجريمة الالكترونية أصبحت تعتمد على أحدث التكنولوجيات (الذكاء الاصطناعي، انترنيت الأشياء...) لتفادي تعقبها ولخلق أكبر ضرر ممكن. وتعتبر المنطقة العربية هشة من هذه الناحية نظرا لاهتمام الشباب، الذين يشكلون أغلبية السكان، بالهجمات السيبرانية وعدم قدرة الأنظمة الالكترونية على مجاراة نسق التطور الكمي والكيفي لهذه الهجمات.

في هذا الصدد، تقترح هذه الوثيقة رؤية استراتيجية لتقليص حدة المخاطر التي تهدد الأمن السيبراني لدول المنطقة العربية.

1.2 الإطار الخاص للدراسة

يندرج إعداد هذه الدراسة في إطار جهود المنظّمة العربية لتكنولوجيات الاتصال و المعلومات و شركائها تنفيذا للقرارات المتعلقة و الهادفة الى رفع مقدرات المنطقة العربية في قطاع تكنولوجيات الاتصال و خاصة تنفيذا لقرار القمة التنموية الاقتصادية والاجتماعية في دورتها العادية الرابعة التي انعقدت ببيروت ، بالجمهورية اللبنانية يوم 20 /01/ 2019 و المتمثل في القرار رقم 56 د.ع (4)– ج 3- 20/01/2019– (النقطة 3) الذي نص على :"تكليف الأمانة العامة بالتنسيق مع المجالس الوزارية المختصة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والخبرات المتوفرة لدى الدول العربية، بدراسة وضع رؤية عربية مشتركة في مجال التكنولوجيا و الاقتصاد الرقمي و الامن السيبراني".

في هذا الإطار تم انشاء فريق الخبراء العرب في مجال الأمن السيبراني من المنطقة العربية و تكليفهم بإعداد هذه الدّراسة بتأطير ومتابعة من المنظمة العربية لتكنولوجيات الاتصال والمعلومات.





.2

الباب الثاني

نطاق العمل والمنهجية

2.1. نطاق العمل

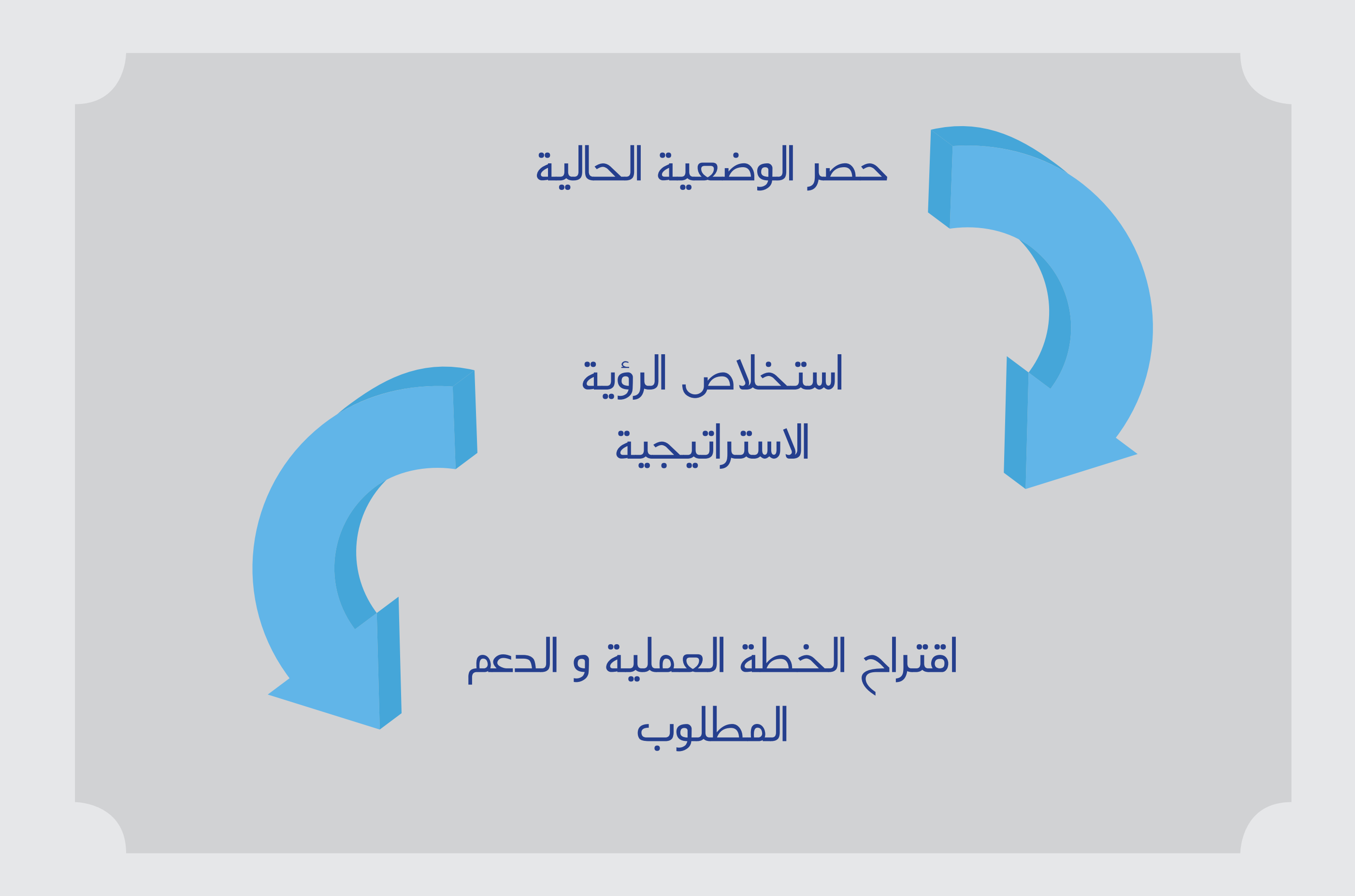
لا شك أنّ المنظّمة العربيّة لتكنولوجيات الاتصال والمعلومات هي أحد الأطراف الفاعلة في مجال الأمن السيبراني على الصّعيد العربي. لذا، ومن منطلق حرصها على تقديم الدعم والمساندة لفائدة الدول العربية تحقيقا لأهداف انشائها، تقترح المنظمة هذه الرؤية العربية للأمن السيبراني التي تهدف الى توفير بيئة تشاركيّة إقليمية لرفع التحدّيات المرتبطة بسلامة وتأمين الفضاء السيبراني.

وقد سعى فريق الخبراء المكلف بإعداد الدراسة إلى تحديد رؤية عامة لتطبيق نظم إدارة الأمن السيبراني وتشغيلها وتحسينها قصد تحقيق قيمة مضافة عبر كمال وشمولية ودقة وصحة وموثوقية البيانات التي توفرها، ومعرفة وتحديد الأخطار المختلفة التي تهدد نظم المعلومات والاتصال، ووضع السبل الكفيلة بحماية البيانات المتضمنة فيها. كما ستمكّن المخرجات المقترحة ضمن هذا العرض من وضع الأسس المرجعية لتحقيق الفوائد التالية:

- إرساء وتطبيق أفضل الممارسات لإدارة نظم أمن المعلومات وضوابطها الأمنية
- صياغة آلية تكامل على الصعيد العربي في مستوى الموارد البشرية والحلول والتطبيقات
- اقتراح سبل لتطوير أدوات تمكين معتمدة على الأمن السيبرني في مجال التحول الرقمي
- توفير وسائل المراقبة والسيطرة على أمن المعلومات، والتقليل من وطأة المخاطر المحدقة بأعمال إدارة المعلومات
- معالجة شاملة لتطوير الهيكل التنظيمي لنظم أمن المعلومات في إطار تطبيق أفضل الممارسات و السياسات وخطط النشاط والمسؤوليات والاجراءات والعمليات
- تحسين قدرة التعامل مع الحوادث الأمنية والتعافي منها بشكل أسرع ومواصلة العمل في حالات الأزمات
- رفع مستوى الوعي بين الموظفين بشأن مفهوم إدارة أمن المعلومات
- زيادة فعالية وكفاءة عملية أمن المعلومات وإدارتها، توفير الوقت والموارد من خلال تفعيل هندسة العمليات

2.2. منهجية العمل

اعتمد فريق الخبراء منهجية مبنية على ثلاث مراحل رئيسية :



اوانطلق فريق الخبراء في حصر الوضعية الحالية على أساس:

- مراجعة الدراسات المقارنة الإقليمية والدولية
- حصر وجمع و تحليل المنشورات و البيانات الرسمية للدول العربية و التدقيق فيها و تحيينها حتى تاريخ عرض الرؤية بتاريخ 21 أكتوبر 2021 الموافق ل09 صفر الثاني 1443ه
- مؤشرات الاتحاد الدولي للاتصالات
- الأطر والمعايير المرجعية القياسية



3.
الباب الثالث
الواقع والتحدّيات

3.1 أهميـة الإطـار القانونـي فـي الرؤيـة العربيـة للأمـن السـيبراني

يعتبـر تركيـز إطـار قانونـي تشـريعي وتنظيمـي ومؤسسـاتي للأمـن السـيبراني مـن أهـم شـروط نجـاح أي رؤيـة أو سياسـة تعمـل علـى ضمان أمن و سلامة الفضاء السيبراني من كل المخاطر السيبرانية والجرائـم التـي ترتكـب فيـه. ويتضمـن هـذا الإطار القانوني الخطـط الإسـتراتيجية والنصـوص والإجـراءات القانونيـة التـي تتعلـق بالإطـار التشـريعي والتنظيمـي أو الترتيبـي و كذلـك الإطـار المؤسسـاتي التـي تسـعى إلـى تحقيـق الهـدف المذكـور أعـلاه.

ويترجـم الإطار القانونـي للأمـن السـيبراني فـي جملـة مـن الخطـط والبرامـج الإسـتراتيجية والقوانيـن سـواء التـي تنقـح وتتمـم القوانيـن الجاري بهـا العمـل أو فـي قوانيـن جديـدة فضـلا عـن اتخاذ اللوائـح والنصـوص الترتيبيـة التـي تأتـي لإنفـاذ هـذه النصـوص التشـريعية. كما يترجـم هذا الإطار القانوني في وضع إجراءات وآليات تنظيميـة وأطر مؤسساتية كفيلـة بتحقيـق إرادة السـلط العمومية في الغـرض بالإضافة إلى وضع آليات للتعاون القانوني خاصة العدلي والقضائي بيـن الـدول لعـدم فاعليـة ونجاعـة الحلـول الوطنيـة لوحدهـا فـي معالجـة المخاطر والجرائـم المرتكبـة فـي الفضـاء السـيبراني.

كما يمكن لنا أن نحصر مجالات التشريع المتعلق بالأمن السيبراني في الأغراض و المحاور التالية: خدمات الثقة الرقمية وخدمات أمن أنظمة المعلومات وخدمات أمن البنى التحتية الحساسة و مكافحة الجريمة السيبرانية و حماية البيانات الشخصية.

و تتمثـل أهميـة الإطار القانوني في تحقيـق الأمن السيبراني بالمقارنة مع الآليات و المبادرات الأخرى في هذه الدراسة، في مساهمته في تحقيـق الأهـداف التاليـة :

- رسـم خطـة اسـتراتيجية يتـم مـن خلالهـا تقييـم الوضـع الحالـي للمخاطـر و تحديـد الأهـداف و البرامـج و الآليـات الكفيلـة بتأميـن الفضـاء السـيبراني.
- وضع القواعد القانونية المتعلقة بتحديد الجرائم السيبرانية والإجراءات المتبعـة في التصدي لها وتتبعها من طرف الجهـاز القضائـي.
- وضـع قواعـد قانونيـة متلائمـة مـع التطـورات التكنولوجيـة التـي يعرفهـا الفضـاء الرقمـي ومـع التهديـدات المسـتجدة التـي يعرفهـا هـذا الفضـاء.
- تمكيـن الهيئـات المكلفـة بتتبـع الجرائـم السـيبرانية مـن إجـراء الأبحـاث والتحقيقـات اللازمـة لذلـك
- وضـع النصـوص التشـريعية واللوائـح الضامنـة لحقـوق الأفـراد وحرياتهـم علـى الإنترنـت أثنـاء إجـراءات التحقيـق فـي الجرائـم الإلكترونيـة ولسـرية بياناتهـم الشـخصية والحافظـة لحياتهـم الخاصـة.
- وضـع الإطار المؤسساتي الـذي تتـم من خلاله مواجهة المخاطر و الجرائم السيبرانية و اتخاذ الإجراءات الأحتياطية اللازمة لحفظ أمن الفضـاء السـيبراني مـن خـلال إحـداث و تنظيـم سـير هيئـة وطنيـة إقليميـة للأمـن السـيبراني و بقيـة المتدخليـن فـي هـذا المجـال.
- وضـع الأسـس التشـريعية والترتيبيـة لمختلـف المبـادرات التـي تعمـل علـى مواجهـة المخاطـر والجرائـم السـيبرانية واتخـاذ التدابيـر الوقائيـة اللازمـة لحفـظ أمـن الفضـاء السـيبراني الوطنـي.
- وضـع الأطـر والإجـراءات والآليـات الكفيلـة بتحقيـق التعـاون القانونـي خاصـة القضائـي بيـن الـدول المعنيـة بالجرائـم السـيبرانية.

3.2 آليـات العمـل العربـي المشـترك فـي مجـال الأمـن السـيبراني

إن اختـلاف وضعيـات الـدول العربيـة وتفاوتهـا فيمـا يخـص اعتمـاد اسـتراتيجية وطنيـة للأمـن السـيبراني والتشـاريع ذات العلاقـة، لـم يمنـع مـن بـروز عـدة مبـادرات علـى مسـتوى العمـل العربـي المشـترك و فـي أطـر تنظيميـة ومؤسسـاتية مختلفـة مـن شـأنها أن تدعـم و تسـاهم فـي تنفيـذ مخرجـات رؤيـة عربيـة للأمـن السـيبراني وخاصـة خطـة عملهـا.

أول هـذه المبـادرات و أهمهـا هـي المصادقـة فـي إطـار جامعـة الـدول العربيـة علـى الإتفاقيـة العربيـة لمكافحـة جرائـم تقنيـة المعلومـات المؤرخـة فـي 2010/12/21 حيـث صـادق عليهـا عـدد مـن الـدول العربيـة الأعضـاء، و دخلـت هـذه الاتفاقيـة حيـز التنفيـذ انطلاقـا مـن تاريـخ 2014/02/06، 30يومـا بعـد مضـي إيـداع وثائـق التصديـق عليهـا و/أو إقرارهـا و/أو قبولهـا مـن سـبع دول عربيـة ملحـق ا.

تهـدف هـذه الاتفاقيـة الـى مكافحـة الجرائـم التـي تعتمـد تقنيـات المعلومـات جرائـم تقنيـة المعلومـات مـع وضـع اطـار للتحقيـق فـي هـذه الجرائـم و ملاحقـة مرتكبيهـا. و رصـدت الأفعـال التاليـة فـي قائمـة الجرائـم التقنيـة:

- الدخـول غيـر المشـروع مـع كل أو جـزء مـن تقنيـة المعلومـات أو الاسـتمرار فيـه.
- الاعتـراض غيـر المشـروع لخـط سـير البيانـات بـأي مـن الوسـائل الفنيـة و قطـع البـث أو اسـتقبال بيانـات تقنيـة المعلومـات.
- الاعتداء على سلامة و سرية و فحوى المعلومات -تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات قصدا بدون وجه حق.
- إساءة استخدام وسائل تقنية المعلومات -انتاج أو بيع أو استيراد أو توزيـع أو توفيـر أو حيـازة أيـة أدوات أو برامـج مخصصـة لغايـة ارتـكاب جرائـم تقنيـة أو شـق كلمـات سـر أو شـيفرة دخـول
- التزويـر
- اسـتخدام وسـائل تقنيـة المعلومـات مـن أجـل تغييـر الحقيقـة فـي البيانـات
- الاحتيـال لتحقيـق المصالـح و المنافـع بطريقـة غيـر مشـروعة باسـتعمال تقنيـة المعلومـات للفاعـل أو للغيـر
- الإباحيـة
- انتـاج أو عـرض أو توزيـع أو نشـر أو شـراء أو بيـع أو اسـتراد مـواد اباحيـة أو مخلـة بالحيـاء بواسـطة تقنيـة المعلومـات
- الأفعال المرتبطة بالاباحية -مقامرة و استغلال جنسي
- الاعتداء على الحرمات الخاصة و سرية البيانات الشخصية
- الإرهـاب -نشـر أفـكار و مبـادئ الجماعـات الإرهابيـة و الدعـوة لهـا و تمويـل العمليـات الإرهابيـة و التدريـب عليهـا و نشـر طـرق صناعـة المتفجـرات و نشـر النعـرات و الفتـن و الاعتـداء علـى الأديـان و المعتقـدات
- الجرائـم المنظمـة
- عمليـات غسـل الأمـوال أو طلـب المسـاعدة أو نشـر طـرق القيـام بغسـل الأمـوال و الترويـج للمخـدرات و أصنافهـا و الاتجـار بالأشـخاص و بالأعضـاء البشـرية و الأسـلحة (غيـر المشـروعة)

- انتهاك حقوق المؤلف
- الاستخدام غير المشروع للأدوات الالكترونية
- الشروع او الاشتراك في ارتكاب الجرائم

وقد اتخذت المبادرات التشريعية العربية المشتركة فيما بعد شكل قوانين إرشادية سواءا في مجال الأمن السيبراني ككل أو في مجال مكافحة الجريمة السيبرانية أو في بعض المجالات الأخرى المحددة مثل القانون الإرشادي العربي في جرائم تقنيات المعلومات و القانون الإرشادي للإثبات بالتقنيات الحديثة و القانون الإرشادي للمعاملات التجارية الإلكترونية و غيرها ... وقد وقع وضعها في إطار أشغال المركز العربي للبحوث القانونية والقضائية التابع لجامعة الدول العربية و الذي يعمل تحت اشراف مجلس وزراء العدل العرب.

وقد اتخذت هذه المبادرات العربية المشتركة شكل مشروع اتفاقية عربية. و في هذا الصدد يمكن أن نذكر إعداد المركز العربي للبحوث القانونية والقضائية مسودة الإتفاقية العربية لحماية الفضاء السيبراني سنة 2018 بمصادقة من مجلس وزراء العدل العرب بجامعة الدول العربية.

و من المفيد ذكر المبادرة حديثة العهد في إطار أشغال لجنة التنسيق العليا للعمل العربي المشترك

الدورة 50- مارس 2021- و التي تم تقديمها من الأكاديمية العربية للعلوم و التكنولوجيا و النقل البحري و المنظمة العربية لتكنولوجيات الاتصال و المعلومات و التي يمكن أن تشكل الإطار المرجعي لمواجهة القرصنة الإلكترونية وحماية الشبكات لمؤسسات ومنظمات العمل العربي المشترك.



3.3 الهياكل المنظمة للأمن السيبراني

من الضرورة التأكيد بداية على أنه في إطار رصد واقع الإطار التشريعي و المؤسساتي للدول العربية في مجال الأمن السيبراني و باعتبار عامل الوقت الذي لم يمكن فريق الخبراء من القيام بجرد كامل محين لهذا الواقع من خلال إجراء استبيان مثلا تشارك فيه كل الدول العربية، فقد خير الفريق سلوك مقاربة نوعية غير كمية تعتمد على أهم الدراسات و المعطيات المتوفرة لديه و تقف على أبرز خصائص هذا الواقع مع ذكر بعض أمثلة من الدول العربية دون البحث على سردها بصفة شمولية و كاملة خاصة و نحن بصدد بلورية رؤية عامة للأمن السيبراني العربي مع التأكيد على ضرورة و أهمية إنجاز دراسة أشمل لواقع هذا الإطار التشريعي و المؤسساتي.

3.3.1 واقع الهياكل الوطنية المتدخلة في الأمن السيبراني

لم تحدث أغلب الدول العربية هيئة وطنية للأمن السيبراني باستثناء بعض الدول التي بعثت مثل هذه الهيئات بتسميات مختلفة: مثل السعودية و مصر وليبيا و الإمارات العربية المتحدة و الأردن و عمان و المغرب و قطر و البحرين و غيرها.

أما في بعض الدول العربية الأخرى، فنلاحظ إحداث مجالس و هيئات عدة لها دور هام في تحديد الرؤية الإستراتيجية الوطنية للأمن السيبراني وفي وضع البرامج العملية لتحقيقها، تتخذ في بعض الأحيان شكل مجالس و في أحيان أخرى شكل هيئات إدارية تابعة لرئاسة الجمهورية أو للوزارة المكلفة بالأمن أو بالدفاع الوطني أو بالعدل مثلما هو الشأن في مصر (المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء) و الجزائر (الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال). أما في الكويت فتباشر الهيئة العامة للاتصالات وتقنية المعلومات الاختصاص المتعلق بمهام ومسئوليات الأمن السيبراني و غيرها....
في مجال حماية البيانات الشخصية، نلاحظ بأن بعض الدول العربية أحدثت هيئات وطنية لمراقبة البيانات الشخصية من ذلك الدول التالية: تونس و الإمارات العربية المتحدة و المغرب و مصر و الأردن. و لكن من المفيد التأكيد على عدم خضوع هذه الهيئات إلى نفس النظام القانوني و عدم تمتعها بنفس الصلاحيات و الإمتيازات مع الملاحظ أن هناك بعض الدول العربية التي أوكلت مهمة مراقبة البيانات الشخصية إلى مصالح وزارة مثلما هو الشأن بالنسبة لدولة قطر، حيث جعل المشرع من الوحدة القانونية لوزارة الإتصالات المصلحة المختصة في هذا المجال ثم بعد ذلك و بمقتضى القرار الأميري رقم ا لسنة 2021 تم نقل مشمولات الأمن السيبراني و حماية البيانات الشخصية إلى الوكالة الوطنية للأمن السيبراني. في دولة الأردن، وقع نشر مسودة مشروع قانون لسنة ٢٠٢٠ لحماية البيانات الشخصية يتضمن إحداث مجلس حماية البيانات الشخصية.

أما في مجال المبادلات الإلكترونية، فأحدثت بعض الدول العربية

هيئة رقابة للمبادلات الإلكترونية و التصديق الرقمي تهتم بتنظيم و إدارة البنية التحتية الوطنية للثقة الرقمية (البنية التحتية للمفاتيح العامة) كتنظيم ممارسة نشاط خدمات الثقة الرقمية و مراقبة تقديم هذه الخدمات و بيان نظام مسؤولية مزودي هذه الخدمات مثل: تونس (الوكالة الوطنية للمصادقة الإلكترونية) و السعودية (المركز الوطني للتصديق الرقمي) و سلطنة عمان (المركز الوطني للتصديق الإلكتروني لإصدار الشهادة الرقمية) و مصر (هيئة تنمية صناعة تكنولوجيا المعلومات) و الجزائر (السلطة الوطنية للتصديق الإلكتروني) و تتجه الأردن وغيرها من الدول إلى إحداث مثل هذه الهيئات...

أما في بعض كما سلكت بعض الدول العربية الأخرى صيغا مؤسساتية مغايرة. ففي الإمارات العربية المتحدة مثلا، تقدم الهيئة الاتحادية للهوية والجنسية خدمة التوقيع الرقمي وخدمات ثقة رقمية أخرى، و في المغرب، تقوم الوكالة الوطنية لتقنين الإتصالات بمهام هيئة رقابة للمبادلات الإلكترونية و التصديق الرقمي.

وفي إطار حرصها على مساندة الدول العربية للنهوض بمجال الثقة اللالكترونية والتصديق الرقمي، بادرت المنظمة العربية لتكنولوجيات الاتصال والمعلومات إلى إطلاق مبادرة "تعزيز الثقة الرقميّة لدعم الاقتصاد الرقمي في المنطقة العربية". وكان أهم مشاريعها، مشروع "الشبكة الإقليمية للثقة الرقميّة" AAECA-Net الذي يهدف إلى المساهمة في تطوير التجارة الالكترونية وتأمين سلامة وسريّة المبادلات الالكترونية". وتتكوّن هذه الشبكة من أصحاب المصلحة المتعدّدين للثقة الرقميّة والتصديق الالكتروني على المستوى الاقليمي. ولديها الخصوصيّة بأنها مفتوحة لجميع العاملين في المجال والمهتمين بالموضوع من حول العالم.

ومن خلال تحقيق رؤية الشبكة الرامية إلى العمل : "نحو مزيد من التنسيق والتعاون الاقليمي والبين الاقليمي في مجال الثقة الرقميّة من أجل اقتصاديات أكثر موثوقية تعتمد على موائمة الأطر القانونية والاعتراف المتبادل لخدمات الثقة الرقميّة"، تساهم المنظمة بذلك في دعم تطوير الاقتصاد الرقمي داخل البلدان العربية الذي يرتكز خاصّة على توفير السلامة والثقة لمستعملي الخدمات الرقمية عبر تنسيق الجهود والتعاون الإقليمي والدولي في مجال الثقة الرقميّة سواء كان ذلك على مستوى الأمن السيبراني أو التصديق الالكتروني.

ومن أهم المخرجات المنتظرة من هذا المشروع :

1. العمل على مواءمة الأنظمة والاعتراف المتبادل بين هياكل المصادقة الالكترونية في الدول العربية من جهة وبينها بين بقية دول العالم من جهة أخرى
2. تنسيق الأطر القانونية والتشريعية والسياسات المتعلقة بالإمضاء الإلكتروني والمصادقة الالكترونية وخدمات الثقة الرقمية بين الدول العربية بالإعتماد على التجارب المقارنة
3. تطوير مشروع إستراتيجية عربية لحث الدول العربية على النهوض بهياكل التصديق الإلكتروني وإرساء آليات التعارف المتبادل بينها وتطوير فضاء مؤمن للمعاملات والمبادلات والتجارة الالكترونية.

وتضم "الشبكة الإقليمية للثقة الرقميّة" في عضويتها ١٠ دول ممثلة في الهياكل الوطنية للتصديق الالكتروني/ الرقمي إلى جانب علاقات شراكة مع الهيئات الدولية المتخصّصة على غرار الشبكة الاقليمية الاسيوية Asian PKI Consortium و "المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية ETSI.

وتأمل المنظمة وتأمل المنظمة أن يتم التفاعل مع هذا المشروع والمشاركة في مختلف أنشطته والانتفاع بالخدمات التي يقدّمها خدمة لتطوير الاقتصاد الرقمي ولوضع الخطط المستقبلية الملائمة للثقة الرقمية بالدول العربية.

3.3.2. واقع استعداد المنطقة العربية في مجال التشريعات

لقد عمدت بعض الدول العربية إلى وضع قانون خاص بالأمن السيبراني يحتوي على مختلف أبعاد هذا الأخير على النحو المكرس في أفضل التشريعات في العالم في هذا المجال أي: نظام قانوني مادي للجريمة السيبرانية و نظام قانوني إجرائي لتتبعها و هيئة تنظيمية و رقابية خاصة و نظام قانوني للتعاون الدولي في الغرض و إطار تعاون داخلي بين مكونات نظام الأمن السيبراني. من بين الدول العربية التي اتخذت لها مثل هذا التشريع يمكن أن نذكر :الأردن (قانون الامن السيبراني رقم 16 لسنة 2019) و المغرب (قانون رقم ٠5.2٠ يتعلق بالأمن السيبراني).

في المقابل، اتجهت بعض الدول العربية فقط إلى وضع قوانين خاصة تتعلق بمكافحة الجرائم المتعلقة بوسائل الإعلام و الإتصال أو بالأحرى بالجرائم السيبرانية مثلما هو الشأن بالنسبة لكل من: السعودية، والإمارات العربية المتحدة والسودان ولبنان و اليمن و الكويت و مصر و البحرين. هناك بعض الدول العربية الأخرى التي أجرت تعديلات على قوانينها الجزائية مثلما هو الشأن بالنسبة لتونس و عمان. كما أن هناك دول عربية أخرى ضمنت الأحكام المتعلقة بمكافحة الجرائم السيبرانية في قانونها العام المتعلق بالأمن السيبراني مثل الأردن و المغرب. كما يمكن أن نلاحظ أن بعض الدول مثل الجزائر قد صادقت على قوانين خاصة بالإجراءات المتصلة بتتبع الجرائم السيبرانية (القانون عدد 2009 ... 4 المؤرخ في 5 أوت 2009 المتعلق بالقواعد الإجرائية الخاصة بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام و الاتصال).

أما في خصوص التشريعات المتعلقة بالمعاملات الإلكترونية، فإن أغلب الدول العربية وضعت مثل هذه التشريعات مثل الأردن و الإمارات العربية المتحدة والبحرين و سوريا و مصر و السعودية و تونس و المغرب و الجزائر و الكويت و البحرين و مصر و غيرها مع الملاحظ بأن أغلب هذه النصوص قد تعلقت كذلك بالتجارة الإلكترونية.على مستوى آخر، صادقت العديد من الدول العربية على قانون يتعلق بحماية البيانات الشخصية من ذلك الدول التالية: الإمارات العربية المتحدة و قطر و تونس و المغرب ولبنان و البحرين و مصر و غيرها. هناك بعض الدول الأخرى التي شرعت في إعداد مشروع قانون يتعلق بحماية البيانات الشخصية دون أن تتوصل إلى المصادقة عليه إلى هذا التاريخ مثل الأردن و جزر القمور مع الملاحظ بأن بعض الدول العربية الأخرى خصصت بعض أحكام قانونها المتعلق بالمبادلات و التجارة الإلكترونية إلى النظام القانوني للبيانات الشخصية مثلما هو الشأن بالنسبة إلى الكويت و سلطنة عمان. أما في المملكة العربية السعودية فقد تم يوم 15 سبتمبر 2021 المصادقة على نظام لحماية البيانات الشخصية يدخل حيز التنفيذ خلال 6 أشهر من تاريخ نشره.

3.3.3 مبادرات الدول العربية المتعلقة بتطوير استراتيجيات وخطط وطنية للأمن السيبراني

رغم أهميتها في ضمان أمن الفضاء السيبراني الوطني، لم يكن اعتماد استراتيجية وطنية للأمن السيبراني قاسما مشتركا بين جميع الدول العربية. وإذ نجد اعتمادها من طرف بعض الدول العربية مثل السعودية و عمان و مصر و الإمارات و الأردن و العراق و لبنان و تونس و المغرب و الكويت، جزر القمور و غيرها، نلاحظ أن بعض الدول العربية الأخرى لا تزال بصدد بحث ومناقشة استراتيجياتها الوطنية في الغرض، مثل الجزائر و موريتانيا. أما البعض الآخر من هذه الدول، فلم تشرع بعد في إعداد هذه الإستراتيجية الوطنية مثل جيبوتي. مع العلم بأن هناك العديد من الدول العربية قد تطرقت لمحور الأمن السيبراني في إطار استراتيجياتها المتعلقة بقطاع الاتصالات وتكنولوجيا المعلومات بصفة عامة على غرار ليبيا -استراتيجية غير مصادق عليها حتى تاريخ اعداد هذه الوثيقة.

وبالإطلاع على فحوى أغلب الإستراتيجيات الوطنية العربية المعمول بها، نلاحظ أن منهجية إعدادها ووضعها و تنفيذها متقاربة لتوفرها على نفس العناصر تقريبا المتمثلة في اعتماد المراحل التالية: الإستهلال و الجرد و التحليل و إنتاج الإستراتيجية الوطنية للأمن السيبراني و التنفيذ و المراقبة والتقييم. كما أن محتواها هو كذلك متقارب باعتبارها تتضمّن المحاور التالية: تحديد المخاطر و التحديات التي تتهدد أمن الفضاء السيبراني و ضبط الأولويات الإستراتيجية و القطاعات الحيوية المستهدفة و رسم الأهداف الإستراتيجية الوطنية و القطاعية و وضع آليات التنفيذ و البرامج الكفيلة بتحقيق هذه الأهداف و وضع آليات لتقييمها. و من بين المحاور الهامة في الإستراتيجية الوطنية يمكن ذكر ما يلي: الإطار التشريعي والتنظيمي و إطار تكنولوجيا الأمن السيبراني و ثقافة الأمن السيبراني وبناء القدرات و الإمتثال والتنفيذ و الجاهزية لحوادث الأمن السيبراني و التعاون الدولي... وبذلك تكون أغلب هذه الإستراتيجيات المعتمدة من طرف بعض الدول العربية متوافقة بشكل كلي مع أفضل الممارسات الدولية في هذا المجال مثلما جاء مثلا في "الدليل لوضع استراتيجية وطنية للأمن السيبراني: التزام استراتيجي بالأمن السيبراني" للإتحاد الدولي للإتصالات أو المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت في الدول العربية لجمعية مجتمع الإنترنتISOC.

3.4 تطور مؤشرات الدول العربية

كان للجهد المبذول خلال السنوات الأخيرة من قبل الدول العربية في بناء القدرات في مجال الامن السيبراني الأثر المتميز، حيث تطور ترتيب العديد من الدول العربية في مؤشرات الاتحاد الدولي للاتصالات المتخصصة. وتميزت في هذا المجال المملكة العربية السعودية التي قفزت في خلال ثلاث سنوات من المرتبة 46 الى المرتبة الثانية عالميا -ترتيب سنة 2020.

هذا التميز تحقق خاصة بإنشائها لمركز وطني للأمن السيبراني و لتبنيها لحزمة كبيرة من السياسات و لمؤشرات قياس الأداء الخاصة بالأمن السيبراني، والمراقبة المستمرة لحالة الأمن السيبراني كما أعتمدت المملكة على المعايير العالمية في مجالات تصنيف البيانات، الحوسبة السحابية، وحماية البيانات، و غيرها... هذا بالإضافة إلى تبنيها للقوانين التي يتم تطبيقها.كما طورت المملكة مجموعة من البرامج والمبادرات للتدريب على موضوعات مختلفة في الأمن السيبراني لاعداد كبيرة جدًا من الموظفين والعاملين في هذا المجال. هذا التطور جاء نتيجة لجهود المملكة في تنفيذ إصلاحات في بيئة الأعمال و البرامج الحكومية في اطار تنفيذها للرؤية الاستراتيجية السعودية ٢٠٣٠ -الهادفة أساسا لتعزيز فاعليتها ولرفع تنافسيتها. بالاظافة الى المملكة العربية السعودية، تطورت مؤشرات كل من الامارات العربية المتحدة و المغرب و البحرين و الكويت. في حيت استقرت نسبيا مؤشرات الدول العربية الأخرى.

و يهدف هذا المؤشر القياسي للاتحاد الدولي للاتصالات الى قياس مستوى التزام كل دولة عضو في الاتحاد إزاء المجالات الرئيسية الخمسة للأمن السيبراني: الجانب القانوني، والجانب التقني، والجانب التنظيمي، وبناء القدرات والتعاون. ويهدف هذا المؤشر إلى مساعدة البلدان في تحديد مجالات التطوير وتحفيز الإجراءات اللازمة لتحسين الترتيب ذي الصلة للرقم القياسي العالمي للأمن السيبراني وزيادة مستوى الأمن السيبراني في العالم أجمع والمساعدة في تحديد وتشجيع أفضل الممارسات وتعزيز بناء ثقافة عالمية في مجال الأمن السيبراني.

3.5 تحليل المخاطر التي تعترض الدول العربية

3.5.1 تقييم المخاطر

تتمحور أهم المخاطر المحدقة بالأمن السيبراني في المنطقة العربية خاصة على المستوى القانوني و المؤسساتي حول النقاط التالية :

- عدم اعتماد العديد من الدول العربية استراتيجية وطنية للامن السيبراني
- عدم اعتماد عديد الدول العربية لتشريع خاص بالأمن السيبراني.
- تبعثر التشريعات المتعلقة بالأمن السيبراني والجرائم السيبرانية بين عدة قوانين وغياب قانون موحد في الغرض يسهل الرجوع إلى أحكامه.
- تعدد الهياكل المعنية بالأمن السيبراني مما خلق صعوبات على مستوى تحديد مجالات تدخل كل واحد منها وعلى مستوى التنسيق بينها.
- عدم ملاءمة بعض التشريعات المتعلقة بالأمن السيبراني لخصوصيات وتحديات الفضاء الرقمي
- عدم ملاءمة بعض التشريعات التي تشكل البيئة القانونية للأمن السيبراني (مثل قانون الاتصالات الإلكترونية ...) مع خصوصيات و



رسم بياني - تطور مؤشر الاتحاد الدولي للاتصالات في الفترة 2017 الى 2020

تحديات الفضاء الرقمي.

- بقاء العديد من القوانين المتعلقة بالأمن السيبراني دون نفاذ لغياب النصوص الترتيبية اللازمة لتحقيقها.
- افتقار معظم الدول الى التشريعات الخاصة بمعالجة وحماية البيانات ذات الطابع الشخصي.
- غياب المرجعية الموحدة بين الدول العربية المعنية بالمسائل التنظيمية والقانونية للفضاء الرقمي.
- نقص كبير في اللوائح التنفيذية والقرارات الإجرائية والأدوات التنظيمية لتطبيق القوانين.
- افتقاد أغلب الدول العربية إلى قانون إجرائي ينظم مسألة التحقيق و جمع الأدلة الإلكترونية لما لهذه الإجراءات من خصوصية بارتباطها بالفضاء الرقمي.
- صعوبات تطبيق القوانين الإجرائية الجزائية التقليدية في الفضاء الرقمي.
- إلتجاء بعض الدول إلى استصدار لوائح ونصوص ترتيبية خاصة في مجال إجراءات تتبع الجرائم السيبرانية نظرا لبطء المسار التشريعي رغم أن مجال هذه النصوص الترتيبية من أنظار المشرع.
- صعوبات قبول الأدلة الرقمية لدى المحاكم سواء المدنية أو الجزائية في ظل عدم الإعتراف القانوني بها في بعض البلدان من حيث الحجية و القيمة الثبوتية.
- قصور الوسائل التقليدية للتعاون الدولي القضائي في تحقيق نجاعة التصدي إلى مسائل الجرائم السيبرانية.
- ضعف الإمكانيات البشرية و المادية في بعض البلدان العربية للتصدي إلى الجرائم السيبرانية
- غياب فرق مختصة لدى الضابطة العدلية للتصدي إلى الجرائم السيبرانية.
- صعوبات حسم مسألة الإختصاص القضائي بالنسبة لجرائم إلكترونية عابرة للحدود الوطنية.
- عدم كفاية برامج توعية المواطنين و عدم تشريك المجتمع المدني في ديناميكيتها.
- التركيز في أغلب الدول العربية على دور الدولة المركزي في تنفيذ مبادرات الأمن السيبراني بما في ذلك في مجال فرق التصدي لحوادث أمن الحاسبات.
- افتقار فرق التصدي لحوادث أمن الحاسبات لأسس قانونية لنشاطها و للموارد المالية والتجهيزات والقوى البشرية والمهارات و التمكين.

3.5.2 التحديات الاقليمية

هناك العديد من التحديات التي تواجه الأمن والاستقرار والازدهار في المنطقة خاصة مع تنامي الاعتماد بشكل كبير على التكنولوجيا وسرعة انتقال المعلومات، ويبرز مفهوم الأمن السيبراني كأحد أهم هذه التحديات على المستوى الإستراتيجي لما له من تأثير وطني ودولي. وتطورت هذه التحديات في ظل الأزمة الصحية العالمية الاستثنائية وغير المسبوقة التي يمر بها العالم منذ بداية انتشار فيروس كوفيد-19 و التي فاقمت بشكل ملحوظ عدد الهجمات المستهدفة لمختلف مكونات الفضاءات السيبرانية. وقد مثلت التغييرات المفاجئة التي طرأت على أساليب ومناهج إسداء الخدمات عن بعد أهم عامل مساهم في تواتر الهجمات الالكترونية وتفاقم المخاطر المحدقة بالأمن السيبرني.

في هذ الإطار، ينبغي على الدول أن تتخذ الدول تدابير دائمة

ومتطورة من أجل ان تكون مستعدة لمواجهة مخاطر التهديدات السيبرانية على بناها التحتية ضمن فضاء معلوماتها الرقمية وما يرتبط بنشاطاتها على مواقع الشبكة العنكبوتية العالمية، وهو ما يستدعي تعزيز وتعضيد مقومات ترسانتها الالكترونية بالاعتماد على عناصر قوتها الوطنية وبالمشاركة مع القطاع الخاص لتفادي عواقب الإضرار بمصالحها الاستراتيجية ومرتكزات أمنها القومي..

ويعيد الفضاء الرقمي تشكيل السياسة والاقتصاد والمجتمعات في جميع أنحاء العالم. حيث تعتمد العديد من هذه المجتمعات والشركات على التشغيل المستمر للآلات الرقمية لتقديم الخدمات الهامة مثل: المستشفيات والتمويل والاتصالات وغيرها من الأغراض العسكرية والمدنية. ونتيجة لذلك، يواجه مستخدمي الإنترنت العديد من التحديات، الامر الذي يتطلب استجابة أمنية على اعلى المستويات لمواجهة تلك التحديات والمخاطر و تقليل الأضرار الناجمة عنها.

أما في ما يتعلق بحماية الفضاء الرقمي من تهديدات الجريمة الإلكترونية والإرهاب السيبراني والهجوم الإلكتروني من قبل الدول أو الجهات الفاعلة غير الحكومية، فإنه يخص حماية الشبكات والأنظمة المعلوماتية من الهجمات التي يمكن أن تعرض الأجهزة أو البرامج أو المعلومات للخطر، سيما وان هذه الهجمات قد تؤدي إلى تسريب معلومات خاصة ، فضلاً عن إلحاق الضرر أو خلق الفوضى لزعزعة الاستقرار والدفع باتجاه زيادة الاضطراب على مختلف الاصعدة : سياسياً، أمنياً، إقتصادياً وعسكرياً.

وعلى الرغم من الفرص الجديدة التي أوجدها الابتكار الرقمي والتي ساهمت بشكل كبير في دفع عجلة التطور التكنولوجي ، إلا أنه ينطوي على تحديات أمنية كبيرة، لعل أعظمها هو تحقيق أمن المعلومات بالإضافة الى إدارة المخاطر ، والتنظيم ، وإدارة البنية التحتية ، والتعافي من الكوارث.

وفي ضوء ما تم ذكره، فلابد من النظر الى مفهوم الفضاء الرقمي وحملات التخريب والتجسس والتعطيل أو الإتلاف وتأثيرها الاستراتيجي على الأمن القومي.

في هذا الاطار يُعَرَّف التعطيل أو الإتلاف بأنه عمل خبيث ومتعمد و غير متعمد يؤدي إلى تعطيل المهام الروتينية والميزات والقدرات الالكترونية، بما في ذلك إلحاق الضرر بالمعلومات والمعدات أو تدميرها.

أما التجسس السيبراني فهو عملية الحصول على المعلومات والأسرار دون إذن من المالك، للحصول على ميزة التفوق على الأفراد والمنافسين والجماعات والحكومات. ويتم تنفيذ عمليات التجسس السيبراني من خلال استغلال خوادم بروكسي عن طريق برامج ضارة ، وفايروسات وديدان، وأحصنة طروادة ، وبرامج تجسس او عن طريق استغلال اي ثغرات امنية اخرى في الانظمة المستهدفة.

ويعرف التخريب بأنه الأنشطة التي تهدف إلى التأثير على السياسات المحلية للبلد المستهدف. و هو نوع من أنواع الحروب الجديدة دون سلاح. ويقوض التخريب السيبراني قوة وسلطة النظام السياسي أو مؤسسات الدولة، ويهدف إلى تحقيق تأثير استراتيجي دون استخدام القوة.

و أصبحت عندئذ شبكة الإنترنت تمثل أرضية ملائمة لممارسة المزيد من الأعمال الإرهابية والعدوانية، أكثر من أي وقت مضى، إضافة إلى التطوّر السريع ومستوى التمكن من التكنولوجيات الحديثة لدى المجموعات الإرهابية. تتعامل هذه المجموعات الإرهابية فيما بينها بطرق لم تكن متاحة في الماضي، وذلك باستغلال وسائل الاتصال الحديثة وخاصة شبكة الإنترنت ، لتأمين التواصل والتنسيق لتعاطي أنشطتهم، وإشاعة أفكارهم، واستقطاب الشباب.

لقد أصبحت المخاطر الإلكترونية جزءا من الحياة اليومية و كلما زادت رقمنة الخدمات و الحكومات كلما أصبحت أكثر عرضة للإصابة و الهجمات. وبالتالي فعلى أجهزة الأمن القومي المتخصصة المشاركة بشكل متزايد في تحديد ومواجهة الاثار الاستراتيجية لقضايا الأمن السيبراني ضمن إستراتيجياتها التي تربط التكنولوجيا الرقمية بالسياسة العامة للدولة من حيث التنظيم والحوكمة.

هذا وقد أصبحت العمليات السيبرانية الهجومية (Offensive Cyber Operations) احد اهم اشكال الحروب بين الدول ليس فقط الكبرى والمتطورة تكنولوجيا ولكن ايضا العديد من دول العالم التي استطاعت امتلاك هذه الادوات نظرا للسهولة النسبية في الحصول عليها والانخفاض النسبي في تكلفة امتلاكها بالقياس علي ادوات الحروب العادية وقد شهد العالم في العشر سنوات الأخيرة تطورا هائلا فيما يتعلق بقدرات الدول المختلفة على احداث اضرار جسيمه بدول اخرى نتيجة هذه الاختراقات السيبرانية وربما يمتد هذا الامر عبر تاريخ طويل من الاختراقات التي امكن تحديد مصدر بعضها ما زال بعضها لم يتم الجزم بمصدره حتى تاريخ كتابه هذا التقرير.

ولقد اعلنت العديد من الدول الكبرى عن مخاوفها من هذه النوعية من الهجمات التي تستهدف ليس فقط سرية بياناتها ولكنها ايضا استطاعت ان تنال من خدمات البنية التحتية الحرجة (Critical Infrastructure) في العديد من الدول. فقد تعرضت كبرى دول العالم الى هجمات طالت انظمه البنية التحتية الحرجة وانظمه التحكم الصناعي (Industrial Control Systems) والخدمات الإلكترونية الحكومية ومحطات تحلية المياه ومحطات توليد الكهرباء وانظمة ادارة الملاحة الجوية بالمطارات ومرورا بأنظمة الإدارة الصحية حيث استطاعت هذه الهجمات الوصول لكل القطاعات وفي كل انحاء العالم ومهما كانت الامكانيات التقنية الدفاعية الخاصة بكل دولة عالية. وتظل القاعدة الرئيسية في امن المعلومات انه "لا يوجد نظام امن ١٠٠٪ " بما يجعل الجميع مستهدف والجميع في دائرة التهديد.

والجدير بالذكر ان الولايات المتحدة الامريكية أعلنت في سبتمبر عام ٢٠١٨ عن استراتيجية الامن القومي السيبراني الأمريكية (National Cybersecurity Strategy) لمجابهة المخاطر التي تتعرض لها. كما أعلنت المملكة المتحدة عن تشكيل قوي سيبرانية بالتعاون ما بين المركز الرئيسي للاتصالات الحكومية (GCHQ) ووزارة الدفاع البريطانية يقدر قوامها ب ٢٠٠٠ هاكر. وفي اكتوبر عام ٢٠١٨ اعلنت قيادة حلف الناتو عن تشكيل مركز التميز لقوة الدفاع السيبراني

المشترك

(CCDCOE - Cooperative Cyber Defence Centre of Excellence) والذي يشارك به ٢٥ دولة في تشكيل مركز على اعلى مستوى من التجهيزات التقنية والمهارات البشرية لرصد الهجمات السيبرانية على اي من الدول الاعضاء للحلف وكذلك التصدي لها محاولة منعها او التقليل من اثارها. وقد بحث الحلف توجيه ضربات عسكرية لأي دولة يثبت تورطها في شن هجمات سيبرانية على أي من الدول الاعضاء ومن المخطط ان يكون هذا المركز في اتم الاستعداد للعمل بحلول عام 2023.

وقد سبقت المانيا وفرنسا الولايات المتحدة الأمريكية وكذلك المملكة المتحدة في الاعلان عن تشكيل جيوش سيبرانية قوامها المعلن ١٣٥٠٠ هاكر واعتبرت وزاره الدفاع الألمانية هذا الكيان ضمن الوحدات الرئيسية في وزاره الدفاع الألمانية شانها شان القوات الجوية والبرية والبحرية واخيرا وليس بآخر فقد اعلنت فرنسا ايضا تشكيل وحدات من الجيوش السيبرانية لمجابهة المخاطر التي تتعرض لها فرنسا من هذه الهجمات.

3.5.3 بعض النماذج الحديثة للاختراقات

في ما يلي بعض النماذج الحديثة للاختراقات لتي كان لها تأثير ضخم على الامن القومي للدول وحماية بياناتها الحساسة او تعطيل خدمات البنية التحتية الحرجة بها:

3.5.3.1 الاختراق العظيم"The Great Hack"

أطلق على هذا الاختراق إسم الاختراق العظيم نظرا لمستوى التعقيد المرتبط به وايضا آلية التنفيذ وكذلك الآثار المترتبة عليه. و بلا منازع هو أحد أهم وأقوى الاختراقات التي حدثت في السنوات الأخيرة حيث تم اختراق احد اكبر الشركات العاملة في مجال انتاج برامج ادارة و مراقبه شبكات وانظمه المعلومات وهي شركه (Solar Winds)التي تملك الالاف من العملاء في كل انحاء العالم ولا سيما بالولايات المتحدة الأمريكية. وبعد اختراق هذه الشركة تمكن المخترقون من استغلال برامجها الموجودة لدى عملائها لاختراق هؤلاء العملاء مما جعل هذا الاختراق متعدد المراحل، لم يكتفي فقط باختراق الشركة المنتجة للبرمجيات بل اتخذها وسيلة لاختراق عملائها. وحتى نتعرف على حجم الاضرار الناجمة عن هذا الاختراق يكفي ان نعلم أن من عملاء هذه الشركة وزارة الخزانة الأمريكية و وزارة الدفاع الأمريكية و شركة مايكروسوفت. وبعد اكتشاف هذا الاختراق أعلنت شركة (Solar Winds) أن هناك 18000 من عملاءها قد تعرضوا لهذا الاختراق ومنهم شركة مايكروسوفت والتي أعلنت بدورها لاحقا عن تعرض 30,000 من عملاء نظام الحوسبة السحابية لديها للاختراق بالتبعية. وقد لا نكون مبالغين بالقول ان حجم الاضرار الفعلية الناتجة عن هذا الاختراق من الضخامة ان تعجز أي جهة ما من حصرها .وتشير تقارير وكالة الاستخبارات الأمريكية ان الفاعل وراء هذه الهجمات هو مخابرات أجنبية وهو ما دعا الرئيس الأمريكي الحالي الى فرض عقوبات قدرها مليار دولار على شركات روسية قال انها متورطة في هذا الاختراق.

3.5.3.2 فضيحة تسريب بيانات ملايين من المواطنين الامريكيين من خلال تطبيقات التواصل الاجتماعي والتأثير على الرأي العام الأمريكي

في سابقة من نوعها استطاعت أحدى الشركات المتخصصة في إدارة الحملات الانتخابية ((Cambridge Analytic والتي كانت أحد الشركات المساهمة في ادارة الحملة الانتخابية للرئيس السابق للولايات المتحدة الحصول على بيانات أكثر من ٨٠ مليون مواطن امريكي. هذه البيانات التحليلية أمكن من خلالها تحديد من هم مؤيدون له ومن هم مؤيدون لمنافسه. وبدراسة البيانات الديموغرافية وتحليل توجهات اصحاب هذه الحسابات السياسية عبر تحليل سلوكهم على شبكات التواصل الاجتماعي أمكن تنفيذ حملات دعائية وتوجيه محتوى يعمد الى تحسين الصورة الذهنية لدي مستخدمي هذه الحسابات لمترشح ويعمد



على إظهار مساوئ المترشح الآخر ولا سيما بعد فضيحة سيبرانية أخرى متعلقة باختراق بريده الالكتروني وافشاء اسرار حرجة للغاية تتعلق بفترة سابقة.

3.5.3.3 اختراق مركز التحكم الرئيسي بكييف - اوكرانيا

في عام 2016 تم اختراق المنظومة الإلكترونية الخاصة لمحطة التحكم الرئيسية بمدينة كييف في اوكرانيا والتي تتبعها اكثر من 60 محطة فرعية، حيث تم اختراق حسابات العاملين في إدارة المحطة و من ثم استغلال كلمات السر الخاصة بهم للدخول عن بعد والتحكم في المحطات الفرعية و الوصول الى الانقطاع التام للتيار الكهربائي. و قد ترتب عن هذا الانقطاع لساعات طويلة العديد من الأضرار على كافة القطاعات سواءا العسكرية أو المدنية ومنها على سبيل المثال لا الحصر : المستشفيات و الخدمات الحكومية الإلكترونية وكذلك تأثيرات شديدة على خدمات القطاع المصرفي و لعله من الضروري ذكر ان هذا الامر تكرر عدة مرات بأشكال و اهداف مختلفة.

3.5.3.4 فضيحة "Crypto AG"

تعد شركه "Crypto AG" أحد أكبر وأشهر الشركات العاملة في إنتاج أجهزه ومعدات التشفير للمراسلات ذات درجات السرية العالية على مستوى رؤساء الدول وكذلك الهيئات الدبلوماسية في كل انحاء العالم. ولعشرات السنوات كانت هذه الشركة تحظى بثقة عشرات الدول حول العالم حيث باعت اجهزتها فيما يزيد على 120 دوله حول العالم. وفي فبراير عام ٢٠٢٠ نشرت جريدة الواشنطن بوست تقريرا صادما حيث اعلنت أنه وقع الاستحواذ على هذه الشركة سرا من طرف دولة متقدمة و قد استطاعت بأساليب تقنية متطورة الحصول على مفاتيح تشفير المستخدمة هذه الأجهزة مما مكنها من رصد ومتابعه كل المراسلات التي تتم عبر أجهزة الشركة في كل انحاء العالم ومن الصادم أن هذا الاختراق بدأ منذ عام 1970. أي انه إمتد عبر ما يزيد على نصف قرن من الزمان بكل ما يحمله من احداث وتفاصيل.

3.5.3.5 اختراق وزاره الصحة البريطانية "National Health Service"

في مايو من عام 2017 تم استهداف وزارة الصحة البريطانية بفيروسات الفدية وتم تشفير بيانات الخوادم الرئيسية العاملة بالمنظومة الصحية وقواعد البيانات والتطبيقات التابعة لها و قد أدى ذلك إلى شلل المنظومة الإلكترونية بالكامل، وكنتيجة لذلك تعطلت كافة الخدمات الصحية في نطاق واسع من المملكة المتحدة، مما كان له بالغ الاثر في إحداث أضرار جسيمه على الخدمات الصحية بالمستشفيات ومراكز الرعاية الصحية وهو ما مثل تهديدا خطيرا على حياة المواطنين المتواجدين أو المترددين على المستشفيات.

مما تقدم، يتبين بوضوح مدى الاضرار البالغة التي يمكن ان تسببها الهجمات السيبرانية وآثارها على الامن القومي للدول. بالنسبة للمنطقة العربية، هناك حاجة ملحة اليوم الى صياغة استراتيجية عربية متكاملة للأمن السيبراني و ذلك من أجل تعزيز التعاون العربي المشترك في هذا المجال الهام وتبادل الخبرات العربية وبناء القدرات، وكذلك من أجل تكثيف التنسيق في رصد ومجابهة المخاطر نحو فضاء سيبرني عربى آمن يمكن العديد من الدول من تحقيق رؤيتها المستقبلية في اتجاه دعم الاقتصاد الرقمي وتنفيذ آليات التحول الرقمي وتقديم الخدمات الرقمية الذكية والمزيد من التوسع في أنظمة الثورة الصناعية الرابعة. بالإضافة إلى تأمين تنفيذ مشروعات المدن الذكية بالعديد من العواصم العربية وهو ما يؤدى في النهاية للحفاظ على الأمن القومي العربي وتقديم مزيد من الرفاهية للمواطن العربي.

3.5.4 تأمين شبكات الهاتف الجوال

3.5.4.1 التحديات

تواجه شبكات الهاتف الجوال من الأجيال الرابعة و الخامسة على غرار كل الشبكات تحديات أمنية وفرصا نابعة عن الخدمات الجديدة التي توفرها بالإضافة الى طبيعة البنية التحتية والتقنيات التي تستغلها ، فضلاً عن المتطلبات العادية لحماية خصوصية وبيانات المستخدم الأخير. و يحتاج كل أصحاب المصلحة إلى فهم متطلبات السيناريوهات المتنوعة لتركيز الشبكات و البنى التحتية و الخدمات المقدمة و خاصة تحديد معايير وتقنيات التأمين بشكل أفضل لمعالجة المخاطر المرتبطة بها.

3.5.4.2 مميزات و فرص التأمين

توفر شبكة الجيل الخامس المستقلة المزيد من ميزات الأمان و السلامة لمواجهة التحديات الأمنية المحتملة في دورة حياة الشبكات المستقبلية ، مثل تأمين الواجهة الراديوية air interface security ، تعزيز حماية البيانات الخصوصية للمستخدم و تعزيز تأمين التجوال و اعتماد خوارزميات تشفير محسنة ، إلخ.

و تشترك شبكات الجيل الخامس غير المستقلة وشبكات الجيل الرابع في نفس آليات الأمان وتعمل وفقًا للمعايير والممارسة باستمرار لمواصلة تحسين مستويات الأمان الخاصة بها. و هي بالتالي شبكات أكثر أمنا من الأجيال الأخرى خاصة من خلال تحقيقها لكل وسائل التأمين المرجعية في كل مكوناتها.

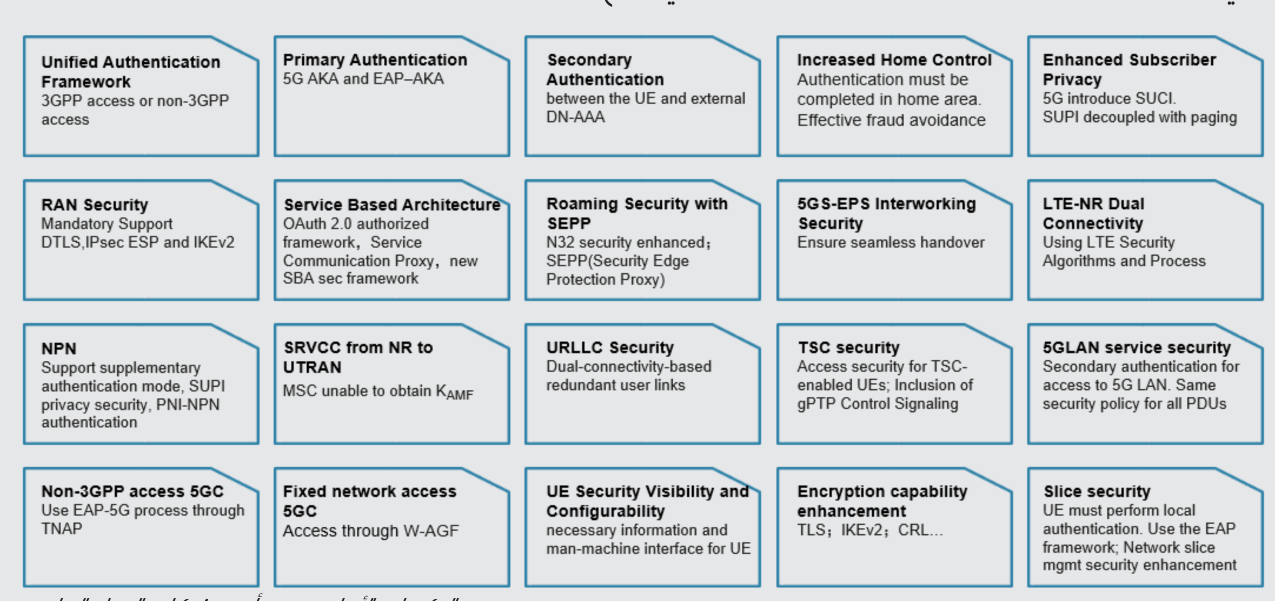
3.5.4.3 معايير قياس السلامة و الأمن

في اطار شبكات الجيل الخامس قامت رابطة- GSMA و هيئة- 3GPP ، المنظمات الرائدة في وضع المعايير في صناعة الاتصالات ، بتعريف مشترك لخطة ضمان أمن معدات الشبكة (NESAS) -و بوضع مواصفات ضمان الأمن (SCAS) للتقييم و التدقيق الأمني لمعدات شبكة الهاتف المحمول. توفر مواصفات NESAS / SCAS اطارا أساسيًا و نهجا موحدا لإثبات والتحقق من أن الشبكات تحقق كل متطلبات الأمن و السلامة.
وقد قامت رابطة المشغلين بإصدار منصة خاصة لتقاسم المعارف في مجال أمن شبكات الجيل الخامس . تهدف هذه المنصة الى مساندة أصحاب المصلحة في تحديد المخاطر وتخطيطها والتخفيف من حدتها؛ و تمثل قاعد بيانات معرفية شاملة لمسح مختلف التهديدات التي تواجه شبكات الجيل الخامس والضوابط والحلول الأمنية المقترحة.

3.5.4.4 بناء الثقة بالشراكة

اليوم، أصبحت شبكات الجيل الخامس حقيقة وستستمر دورة حياة هذا الجيل لبعض الوقت. و استنادًا إلى التجارب الناجحة لتأمين الجيل الرابع، يمكن التحكم في مخاطر أمن شبكات الجيل الخامس من خلال الجهود المشتركة لجميع أصحاب المصلحة.
و قصد بناء نظام يمكن الوثوق به ، هناك حاجة الى العمل في اطار مسؤوليات منسجمة ومعايير موحدة مع إطار تنظيمي واضح.
وللتحكم في مخاطر دورة حياة الجيل الخامس، هناك حاجة إلى تعزيز الحلول الأمنية باستمرار من خلال الابتكار التكنولوجي وبناء أنظمة وشبكات آمنة بالاعتماد على المعايير المناسبة و بالتعاون بين كل أصحاب المصلحة:

- مصنعي الشبكات: يجب على المصنعين المساهمة بجدية في وضع و تحسين المعايير القياسية المؤمنة للشبكات كما يجب عليهم

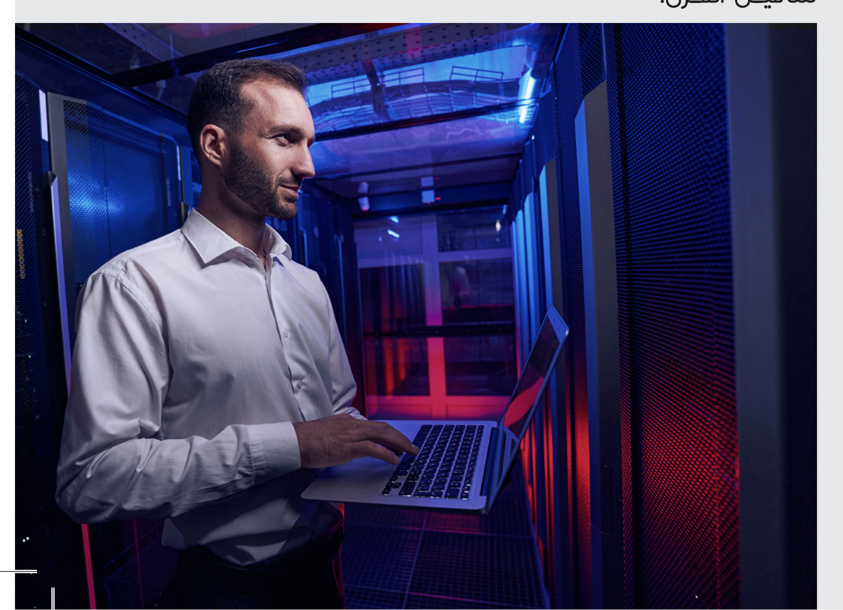


المكونات الأساسية في تأمين شبكات الجيل الخامس

الامتثال للمعايير، ودمج تقنيات التأمين لبناء شبكة آمنة، جنبًا إلى جنب مع العملاء وأصحاب المصلحة الآخرين . و يجب على المصنعين حشد الإمكانيات لدعم المشغلين لضمان التشغيل الآمن و المرن للشبكة.

- المشغلون: المشغلون مسؤولون عن عمليات التأمين المرن المتواصل لشبكاتهم الخاصة. و يمكن للمشغلين منع الهجمات الخارجية بإنشاء جدران الحماية وبوابات الأمان. أما بالنسبة للتهديدات الداخلية، فيمكن للمشغلين وضع الإجراءات المناسبة و الفعالة لإدارة ومراقبة وتدقيق جميع الشركاء للتأكد من أن كل عناصر الشبكة الخاصة بهم آمنة.
- الهيئات التنظيمية الصناعية والحكومية: تحتاج كل هذه الهيئات إلى العمل معًا وفقًا للمعايير القياسية المرجعية في ظل مسؤولية مشتركة. فيما يتعلق بالتقنيات و توجهات الجيل الخامس، هناك حاجة الى وضع سياق مستمر لعزيز تأمين شبكات الجيل الخامس في ظل المخاطر المتعلقة بسيناريوات الخدمات المتعددة (كالتقطيع - Slicing وMEC و mMTC وغيرها). أما فيما يتعلق بضمان التأمين، فهناك حاجة إلى توحيد متطلبات الأمن السيبراني والتأكد من أن هذه المعايير قابلة للتطبيق ويمكن التحقق منها لدى كل المشغلين و المصنعين بالتركيز على تحديد المخاطر والاستجابة لها.

في عصر الجيل الخامس والذكاء الاصطناعي ، يجب على كل أصحاب المصلحة التعاون لوضع المعايير القياسية المرجعية لتأمين الشبكات و لوضع أنظمة التحقق و تحديد المخاطر و الاستجابة لها، مع العمل على ابتكار و تطوير الحلول الجديدة للتأمين المرن.





4.

الباب الرابع

الرؤية الاستراتيجية

4.1. بيان الرؤية الاستراتيجية

نحـو مجتمـع عربـي آمن-متكامـل ومندمـج فـي الاقتصـاد الرقمـي العالمـي و محقـق للاكتفـاء الذاتـي فـي مجـال الحلـول و الخبـرات الداعمـة للثقـة الرقميـة و الحاميـة للفضـاء السـيبراني العربـي

- مجتمع عربي آمن: مجتمع عربي آمن من خلال توفير الشروط والمتطلبـات الموضوعيـة لتحقيـق الامـن السـيبراني و تعزيـز شـعور كافة افراد المجتمع بالامان
- متكامل: شامل و معتمد على تفاعل كل اصحاب المصلحة.
- مندمج في الاقتصاد الرقمي العالمي : من خلال صياغة تدابير السلامة التنظيمية والتقنيـة اللازمة ضد الأضرار المحتملة على ضوء المعايير و أفضل الممارسات الدولية المعتمدة والمبادئ التوجيهية الواضحـة التـي تمكـن الشـركات و الفاعليـن الاقتصادييـن أن تعمـل مـن خلالها بأمـان فـي تطويـر منتجـات وخدمـات رقميـة جديـدة ومبتكـرة تكـون جزءا من الاقتصـاد الرقمي.
- محقـق للاكتفـاء الذاتـي فـي مجـال الحلـول: مـن خـلال وضـع الإسـتراتيجيات التحفيزيـة لمطـوري الحلـول فـي المنطقـة العربيـة من أجل انتاج وسائل وبرامج للسلامة المعلوماتية محلية الصنع.
- الخبرات الداعمة للثقة الرقمية: من خلال وضع البرامج التعليمية و التدريبيـة المؤهلـة للكـوادر و الإطـارات العربيـة فـي كل المجـالات الداعمة للثقة الرقمية.
- الحاميـة للفضـاء السـيبراني/الرقمي العربـي: الهـدف النهائـي الاستراتيجي هو حماية الفضاء السيبراني الإقليمي و الوطني العربي.

4.2. الأهداف النوعية للرؤية

بالنظر الى ما تمت الإشارة اليه من تحديات جدية والمخاطر التي تعترض المنطقة العربية و التي تضاعفت نتيجة للأزمة الصحية العالمية "الاستثنائية" سنة ٢٠٢٠، تهدف هذه الرؤية الى :

- خلـق آليـات تشـاركية مـن خـلال الاسـتفادة مـن سـوق الأمـن السـيبراني فـي المنطقـة
- تطويـر قـدرات المتخصصيـن فـي الأمـن السـيبراني، وتشـجيع المهنييـن والطلبـة علـى الانخـراط فـي المجـال و بنـاء القـدرات وتطوير منظومة متكاملة في مجال التدريب في الأمن السيبراني.
- زيادة وعي أفراد المجتمع بالأمن السيبراني والمخاطر المتعلقة بالإنترنـت، وتشـجيع اتبـاع الممارسـات الآمنـة فـي التعامـل مـع التكنولوجيا الرقمية، وتشجيع المؤسسات على نشر الوعي السيبراني بفاعليـة.
- تنظيم مسابقات تدعم التميز في مجال الأمن السيبراني من خلال برامج الجوائز العربيـة، وتشجيع المؤسسات على إطلاق برامج حول الأمن السيبراني، وإلهام رواد الأعمال للابتكار في المجال، ودعم الأبحـاث الخلاقـة فـي المؤسسـات الأكاديميـة، وتنشـيط تشـجيع الطلبـة على الانخـراط في مجال الأمن السـيبراني.
- تنظيم آلية الكشف عن حوادث الأمن السيبراني والإبلاغ عنها.
- إنشاء منهجية موحدة لتقييم درجة خطورة الحـوادث السيبرانية لتوفير الدعم المناسب لها.
- بنـاء قـدرات عربيـة علـى مسـتوى عالمـي للاسـتجابة للحـوادث السـيبرانية مـع مراعـاه التطـور الهائـل فـي هـذا الشـأن
- تصميم إطار قانوني وتنظيمي شامل للأمن السيبراني لمعالجة جميع أنـواع الجرائم السيبرانية، وبناء إطار تنظيمي لحماية التقنيات الحاليـة والناشـئة، ووضـع أنظمـة داعمـة لتمكيـن الشـركات الصغيـرة والمتوسـطة وحمايتها من التهديدات السيبرانية

4.3. آليات و مقومات وضع الرؤية

من خلال حصرنا لواقع و تحديات الأمن السيبراني بالدول العربية فاننـا يمكـن أن نقـف علـى بعـض المكاسـب التـي يمكـن أن تمثـل المقومات التي سترتكز عليها الرؤية الستراتيجية و تتمثـل في ما يلـي:

- اتجاه العديـد من الـدول العربيـة نحـو اعتمـاد استرتيجية وطنيـة للأمن السيبراني
- اتجاه العديـد من الـدول العربيـة نحـو اعتمـاد تشريع عام للأمن السيبراني
- أهمية المبادرات العربية في تقريب التشريعات الوطنية العربية مـن بعضهـا البعـض وتطويـر العمـل المشـترك فـي مجـال الأمـن السيبراني
- اعتمـاد أغلـب الـدول العربيـة سـواء فـي وضـع الإسـتراتيجية أو التشـريعات الوطنيـة للأمـن السـيبراني علـى أفضـل الممارسـات التشـريعية فـي العالـم.
- تثميـن دور مبـادرات المنظمـات الدوليـة العالميـة و العربيـة بالتحديـد فـي بلـورة اسـتراتيجيات و تشـريعات وطنيـة ناجعـة.



5.

الباب الخامس

الخطة العملية

5.1 الخطوط العامة للخطة العملية

5.1.1 تطوير وتنفيذ استراتيجية وطنيه للأمن السيبراني

تفتقد عديد الدول العربية لوجود استراتيجية وطنيه للأمن السيبراني وهو ما يعكس عدم وجود رؤيه واضحة أو بعيده المدى للمخاطر السيبرانية وكذلك الاهداف الاستراتيجية المطلوب تحقيقها. ويعد تطوير استراتيجية خاصة بالتعامل مع الامن السيبراني هو أولى خطوات العمل نحو تحقيق فضاء رقمي آمن لأية مؤسسة أو دولة ومما لا شك فيه أن مسار هذه الاستراتيجية يبدا بعد ان تحدد كل دولة الرؤية والرسالة الخاصة بها فيما يتعلق بإدارة ملف الامن السيبراني و تأثير مخاطره عليها. و من أهم وأفضل المرجعيات العالمية في هذا الصدد هو النموذج الارشادي الذي تم تطويره من قبل الاتحاد الدولي للاتصالات والمتعلق بخطوات صياغه وتطوير الاستراتيجيات للأمن السيبراني (GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY)
وبمجرد تحديد الرؤية والرسالة ينبغي البدء في إنجاز تحليل الفجوة ما بين الوضع القائم والوضع المرجو الوصول اليه، ثم تطوير الاستراتيجية لتكون بمثابة خارطة الطريق نحو التحرك الى الوضع المنشود. ويجب ان تنفذ استراتيجية الأمن السيبراني في إطار من الحوكمة المؤسسية بما يضمن تقليل المخاطر وحسن استغلال الموارد ، وتوافق المبادرات والمشروعات مع الاهداف لتقديم المخرجات المنتظرة .كما يجب وضع وتطوير معايير لقياس الأداء في كافة المراحل.

كما ينصح وبشدة إتباع أحد الأطر العالمية للأمن السيبراني حيث تمثل هذه الأطر أفضل الممارسات العالمية لإدارة هذا الموضوع المهم ومن أشهر هذه النماذج هو إطار (NIST Cybersecurity Framework) للأمن السيبراني والذي يعمل على خمس محاور متوازية من أجل امتلاك القدرات الكاملة للأمن السيبراني وهي:

1- تحديد الاصول الرقمية والمخاطر المرتبطة بها
2- الحماية والتامين
3- اكتشاف الهجمات السيبرانية
4- الاستجابة للحوادث السيبرانية
5- التعافي من الحوادث السيبرانية

والجدير بالذكر أن الإطار المذكور هو إطار عام يمكن استخدامه في أي مكان وفي اي قطاع من قطاعات الاعمال المختلفة، كما انه لا يرتبط بتكنولوجيا محددة بل يتوافق ويتكامل مع عدد كبير جدا من أشهر المعايير والأطر العالمية المرتبطة بالأمن السيبراني. ويجب أن يرتبط تنفيذ هذا الإطار بوجود العديد من الآليات ومنها على سبيل الذكر لا الحصر ما يلي:

- آلية لتحديد الاصول الرقمية الحرجة للمؤسسة
- آلية لتقييم المخاطر
- آلية لتقييم التأثير على الاعمال
- آلية لدعم مبدا التحسين المستمر

5.1.2 دعم البحث والتطوير

من أهم العوامل والمحاور الداعمة لتحقيق نجاح ملموس في مجال إمتلاك قدرات سيبرانية سواءا في إطار الدفاع أو الهجوم السيبراني هو عامل البحوث والتطوير، ويرتبط مستوى النجاح في تحقيق القدرات المطلوبة بحجم الانفاق والدعم اللوجيستي المتاح للقائمين على البحوث والتطوير في هذا المجال والذي تعددت فروعه وتخصصاته بشكل كبير جدا ومنها على سبيل المثال (الحوسبة السحابية - انظمه الهواتف المحمولة - النظم والتطبيقات الافتراضية - الأنظمة المدمجة وتطبيقات انترنت الأشياء).

ومن الواجب في هذا الصدد القاء الضوء على فرص التشارك المطلوب ما بين القطاع الحكومي الخاص والذي يمكنه تعزيز إستثمارات هذا المجال بما يؤدي إلى تحقيق أهداف عديدة لا تقتصر فقط على دعم البحوث والتطوير وإنما يمكن أيضا أن تنشئ فرص لتطوير حلول وتطبيقات أو وأجهزه تدعم الامن السيبراني وايضا تثري سوق التكنولوجيا في البلدان العربية.

5.1.3 التدريب والتوعية

اي منظومة ناجحة تعتمد على ثلاثة محاور رئيسية (الافراد - الضوابط والسياسات والقوانين - تكنولوجيا). و في مجال الامن السيبراني تعد الموارد البشرية من أهم عناصر المنظومة وتكاد تكون الاهم على الاطلاق. فمهما كانت مقدرة المؤسسات والدول على إمتلاك تقنيات فائقة التطوّر، سيظل الحصول عل أفضل أداء ممكن من هذه التقنيات مرهون بالقدرات على تشغيلها وإدارتها. وهنا تكمن الأهمية الشديدة لإعداد الكوادر وبناء القدرات البشرية. والجدير بالذكر أن العالم يشهد نقصا كبيرا في الكوادر المدربة والمؤهلة لتامين آلاف التقنيات الموجودة في كافه قطاعات الاعمال، مثل : التعليم والصحة و الخدمات الحكومية الإلكترونية و الخدمات البنكية بأنواعها المختلفة و انظمه التحكم الصناعي وشبكات إداره البنيه التحتية الحرجة والتي قد تعد الاخطر على الاطلاق، حيث ان العبث بإعدادات هذه الشبكات او الاتصال غير المشروع بها قد يؤدي الى شلل تام بالمؤسسات بل وبالدول أيضا.

وفي هذا الصدد، يوجد نماذج واطر عالميه شهيرة يمكن الاعتماد عليها أو حتى اعتمادها كما هي من أجل وجود رؤية لإعداد متخصصين في مجالات الامن السيبراني المختلفة. ولعل أشهر هذه النماذج هو نموذج - National Initiative for Cybersecurity Education) (NICE والذي تم تطويره قبل المعهد القومي الامريكي للمعايير القياسية والتكنولوجيا (NIST) .ويحدد هذا الاطار عدد من العملة في مجال الامن السيبراني ويضع لكل وظيفه نوع من التوصيف الوظيفي بالإضافة الى القدرات والمهارات المطلوبة لشاغل الوظيفة، وهو ما يمكن من العمل على إعداد برامج تدريبيه متخصصه بغرض إعداد متخصصين فروع الامن السيبراني المختلفة .كان يضع مسارا واضحا لتطوير قدرات العاملين في

هذا المجال من المستويات الأولى إلي مستويات متقدمة. ولعل أفضل النماذج العربية في هذا الاطار هو ما قامت به المملكة العربية السعودية فيما اطلق عليه : "الإطار السعودي لكوادر الأمن السيبراني (سيوف)".

وإذا كنا نتحدث عن العامل البشري كأحد أهم العوامل الداعمة لنجاح منظومة الامن السيبراني، فإنه لا يقف عند حدود متخصصي ومسئولي الامن السيبراني بل يمتد الى كل فرد في المؤسسة، حيث ومن الوارد جدا ان يتم استهداف أي مؤسسة بالكامل عن طريق أي موظف او منتسب لها، أو حتى أي فرد تعامل مع هذه المؤسسة مثل : الموردين والعملاء والشركاء واي مؤسسة اخرى ترتبط بالهدف المراد اختراقه. ومن هنا تأتي التوعية بمخاطر الامن السيبراني كعامل شديد الأهمية، حيث أننا دائما نقف على أن الحلقة الاضعف في سلسلة أمن المعلومات هي العامل البشري.

وكما تنص كل المعايير العالمية التي تتعامل مع أمن المعلومات وتشترط إعداد برامج توعيه للموظفين او المتعاملين مع المنظومات التكنولوجية بشكل عام ومن هذه المعايير على سبيل الذكر لا الحصر :

- PCI .. Payment Card Industry Standard
- GDPR .. General Data Protection Regulation
- International Standard for Information Security ٢٧٠٠١ ISO

5.1.4 معايير التامين

يعد اعتماد معايير محددة للأمن السيبراني كحد أدنى لضوابط تامين المنظومات التكنولوجية أمرا هاما، ولذا طورت العديد من دول العالم معايير وضوابط قياسيه ملزمه لتحقيق حد أدني من اهداف الامن السيبراني، والتي من الممكن تعزيزها ولكن لا يمكن النزول دونها. ومن أشهر النماذج العالمية في هذا الصدد نموذج الولايات المتحدة الأمريكية

- FIPS Federal Information Processing Standards
- CC Common Criteria
- Security and Privacy Controls for Information) r5 53-800 NIST Systems

كما يوجد أيضا العديد من النماذج العالمية والتي تمثل معايير عامه لا ترتبط بدولة بعينها وانما يمكن إستخدامها كمرجعيات عامه تحظى على قبول من كل المتخصصين في العالم :

- CIS Controls - Top Critical Controls
- International Standard for Information Security 27001 ISO

ومن النماذج العربية المميزة في هذا السياق : الامارات العربية المتحدة والمملكة العربية السعودية وقطر، حيث يوجد في كل من هذه الدول ضوابط ملزمة لقطاعات الاعمال المختلفة بما يكفل تحقيق حد أدني من الامن السيبراني على مستوى الدولة بالكامل، كما يؤسس لتطوير ضوابط أكثر تخصصا وفي كل قطاع من قطاعات الاعمال، أو أكثر قوة وفق متطلبات التامين الفعلية.

5.1.5 التعاون الدولي (التعاون العربي المشترك)

إن تبادل الخبرات والمعلومات التقنية المرتبطة بتحليل آليات الاختراق السيبراني ومحاوله معرفة مصدره واهدافه يعد من الامور الهامة والتي يمكن ان تكون احدى ثمار التعاون العربي المشترك. إذ أن الحصول على المعلومات وتوقيت الحصول عليها هو أمر بالغ الأهمية في اكتشاف الحوادث السيبرانية أو توقع حدوثها. وقد يمكن ايضا من منعها او الحد من اثارها. وفكرة التعاون وتبادل المعلومات ليست جديدة، ولعل من اقوى الأمثلة في هذا الصدد : نموذج حلف شمال الاطلسي الذي انشئ مركز تميز للدفاع السيبراني المشترك من الدول الاعضاء في الحلف. ويضم هذا المركز في عضويته متخصصين من ٢٥ دولة مختلفة و يعمل على رصد التهديدات السيبرانية التي تتعرض لها اي دوله من دول الحلف كما يقوم بمحاولات صد هذه الهجمات بالتنسيق مع كل الدول المعنية من أجل من منعها أو تقليل تأثيرها. وحتى يكون هذا التعاون مثمر وفاعل فإنه يجب ان يغطي المحاور الثلاثة

- الافراد
- السياسات والاجراءات والقوانين
- امتلاك التقنيات المناسبة

كما انه من الممكن مشاركة بعض المعلومات التقنية كنتجة لهذا التعاون مع المراكز البحثية ذات الصلة في الدول العربية بما يعزز قدرتها البحثية وتطوير أدواتها في التصدي للهجمات السيبرانية.

5.1.6 انشاء وتطوير المراكز الوطنية للاستجابة للحوادث السيبرانيه

تعتبر المراكز الوطنية للاستجابة للحوادث السيبرانية بمثابة خط الدفاع الاول أو وحدات الكشف المبكر عن الهجمات السيبرانية. و تلعب دورا هاما في محاولة تحديد مصادر هذه الهجمات واهدافها و محاولة تحليل اساليب عملها و الثغرات المستهدفة بهذه الهجمات، وفي اقل التقديرات ينبغي ان يكون هناك على الاقل مركزا واحدا على مستوى الدولة ويفضل التنسيق بين هذا المركز والمراكز المشابهة والتي تعمل في نطاق محدود علي مستوي مؤسسه بعينها او إحدى الوزارات . كما ينصح بإنشاء مراكز متخصصة على مستوى قطاعات الاعمال المختلفة مثل : قطاع الصحة او الاتصالات او قطاع البنيه التحتية الحرجة، ... حيث يوجد متطلبات نوعيه تختلف من قطاع الى اخر كما تختلف اولويات الهجمات السيبرانيه ووسائلها واهدافها من قطاع الى اخر ومن مؤسسة الى أخرى. وتوجد مراكز الاستجابة للحوادث السيبرانية بالعديد من الدول العربية ولكنها تتفاوت في مقدراتها و إمكانياتها كما أنها تكاد تفتقد لآليات للتعاون العربي المشترك و لتبادل الخبرات والمعلومات. وفي عدد من الدول لا يوجد مثل هذه المراكز وهو ما يتطلب بالضرورة وضع خطة عاجلة لدعم انشاء مراكز الاستجابة الوطنية الحوادث السيبرانية بهذه الدول وكذلك تدريب العاملين بها. وهناك العديد من المرجعيات الدولية التي

يمكن الاستعانة بها في هذا الصدد وعلى رأسها اصدارات الاتحاد الدولي للاتصالات المتعلقة بهذه المراكز وأيضا المركز الاوروبي للأمن السيبراني European Union Agency for Cybersecurity... ENISA وكذلك المعهد القومي المعايير القياسية والتكنولوجيا بالولايات المتحدة الأمريكية. تعتبر المراكز الوطنية للاستجابة للحوادث السيبرانية بمثابة خط الدفاع الاول أو وحدات الكشف المبكر عن الهجمات السيبرانية. و تلعب دورا هاما في محاولة تحديد مصادر هذه الهجمات واهدافها و محاولة تحليل اساليب عملها و الثغرات المستهدفة بهذه الهجمات، وفي اقل التقديرات ينبغي ان يكون هناك على الاقل مركزا واحدا على مستوى الدولة ويفضل التنسيق بين هذا المركز والمراكز المشابهة والتي تعمل في نطاق محدود علي مستوي مؤسسه بعينها او إحدى الوزارات . كما ينصح بإنشاء مراكز متخصصة على مستوى قطاعات الاعمال المختلفة مثل : قطاع الصحة او الاتصالات او قطاع البنيه التحتية الحرجة، ... حيث يوجد متطلبات نوعيه تختلف من قطاع الى اخر كما تختلف اولويات الهجمات السيبرانيه ووسائلها واهدافها من قطاع الى اخر ومن مؤسسة الى أخرى. وتوجد مراكز الاستجابة للحوادث السيبرانية بالعديد من الدول العربية ولكنها تتفاوت في مقدراتها و إمكانياتها كما أنها تكاد تفتقد لآليات للتعاون العربي المشترك و لتبادل الخبرات والمعلومات. وفي عدد من الدول لا يوجد مثل هذه المراكز وهو ما يتطلب بالضرورة وضع خطة عاجلة لدعم انشاء مراكز الاستجابة الوطنية الحوادث السيبرانية بهذه الدول وكذلك تدريب العاملين بها. وهناك العديد من المرجعيات الدولية التي يمكن الاستعانة بها في هذا الصدد وعلى رأسها اصدارات الاتحاد الدولي للاتصالات المتعلقة بهذه المراكز وأيضا المركز الاوروبي للأمن السيبراني European Union Agency for.. ENISA Cybersecurity وكذلك المعهد القومي المعايير القياسية والتكنولوجيا بالولايات المتحدة الأمريكية.

5.1.7 رابط الدراسات الأكاديمية باحتياجات سوق العمل

الى حد بعيد توجد فجوة كبيرة ما بين ما يدرسه طلاب الجامعات من التخصصات التقنية او في مجال أمن المعلومات، ان وجد كتخصص اكاديمي، و بين احتياجات سوق العمل الفعلية. وسيكون التوجه نحو توفير تخصصات دراسية مرتبطة بعلوم الامن السيبراني احد الخطوات الهامة لتوفير كوادر مدربة لسد العجز الشديد ما بين احتياجات سوق العمل وعدد الافراد المؤهلين بشكل مناسب لشغل هذه الوظائف. حيث يمكن توفير اعداد كبيره مدربة بشكل جيد في فتره زمنية قصيرة وايضا بتكلفة قليلة بالمقارنة مع تكاليف التدريب المتخصص أو الدورات المعتمدة عالميا والتي عادة ما يصل سعرها الى بضعة الاف من الدولارات للدورة الواحدة لكل متدرب.

كما يمكن ايضا تطوير محتوى يقوم على اعداده والاشراف عليه نخبة من الاكاديميين والمهنيين من أجل انتاج مناهج دراسية بتكاليف مناسبة لإعداد اجيال من المتخصصين في الامن السيبراني للوفاء بمتطلبات سوق العمل في المنطقة العربية من ناحية، ومن ناحية اخرى لدعم جهود البحث العلمي في هذا المجال الهام. وباستثناء عدد محدود للغاية من الجامعات العربية فإن الغالبية العظمى منها تفتقد وجود تخصصات متعلقة بالأمن السيبراني وربما أيضا لبعض المواد الدراسية المتعلقة بهذا الصدد.

الى حد بعيد توجد فجوة كبيرة ما بين ما يدرسه طلاب الجامعات من التخصصات التقنية او في مجال أمن المعلومات، ان وجد كتخصص اكاديمي، و بين احتياجات سوق العمل الفعلية. وسيكون التوجه نحو توفير تخصصات دراسية مرتبطة بعلوم الامن السيبراني احد الخطوات الهامة لتوفير كوادر مدربة لسد العجز الشديد ما بين احتياجات سوق العمل وعدد الافراد المؤهلين بشكل مناسب لشغل هذه الوظائف. حيث يمكن توفير اعداد كبيره مدربة بشكل جيد في فتره زمنية قصيرة وايضا بتكلفة قليلة بالمقارنة مع تكاليف التدريب المتخصص أو الدورات المعتمدة عالميا والتي عادة ما يصل سعرها الى بضعة الاف من الدولارات للدورة الواحدة لكل متدرب.

كما يمكن ايضا تطوير محتوى يقوم على اعداده والاشراف عليه نخبة من الاكاديميين والمهنيين من أجل انتاج مناهج دراسية بتكاليف مناسبة لإعداد اجيال من المتخصصين في الامن السيبراني للوفاء بمتطلبات سوق العمل في المنطقة العربية من ناحية، ومن ناحية اخرى لدعم جهود البحث العلمي في هذا المجال الهام. وباستثناء عدد محدود للغاية من الجامعات العربية فإن الغالبية العظمى منها تفتقد وجود تخصصات متعلقة بالأمن السيبراني وربما أيضا لبعض المواد الدراسية المتعلقة بهذا الصدد.

5.1.8 تطوير هياكل الإدارية بالمؤسسات

إن من اكبر المشاكل والتحديات التي تواجه معظم الدول العربية هي عدم وجود تحديد لمفهوم الامن السيبراني وكذلك تحديد اين تقع مسئوليات تامين المعلومات والنظم فقد تكون مسؤولية المعلومات هي مسئولية شخص واحد داخل مؤسسة أو فريق عمل تابع لإدارة تكنولوجيا المعلومات، و في حالات نادرة ما تكون ادارة الامن السيبراني اداره موجوده ولها تبعيه مباشرة للادارة العليا .و يمثل هذا النموذج الاخير افضل الممارسات العالمية في هذا الصدد و حين يتعلق الامر بوضع رؤية موحدة للدول العربية بخصوص الامن السيبراني فانه من الضروري أن يكون هناك بكل الهيئات و المؤسسات التابعة للدولة إدارة خاصة بأمن المعلومات و لها مهام واضحة ومحددة بالإضافة الى تشكيل هيكل اداري بهذه الإدارة بتوصيف وظيفي مناسب حتى يكون لكل مؤسسة ادارة تعمل على تامين كل ما لديها من أجهزة رقمية. وتخضع هذه الإدارة والعاملين بها لتقييم الاداء من خلال مؤشرات أداء محددة وتكون في حاله تطوير وتحسن مستمر. ويجب أن تكون تبعية هذه الإدارة لاعلى سلطة داخل المؤسسة بما يدعم ادواتها التنفيذية لتفعيل سياسات وادوات وضوابط الامن السيبراني.

5.1.9 الجانب القانوني

لوضع الرؤية الإستراتيجية الوطنية للأمن السيبراني حيز التنفيذ في جانبها القانوني يجب تحقيق البرامج و اتخاذ الإجراءات و الآليات العملية التالية:

- مراجعة الاستراتيجيات الحالية بما يضمن موائمتها للتغيرات المتسارعة في مجال الامن السيبراني.
- الإسترشاد في عملية تحديث التشريع المتعلق بالأمن السيبراني بأفضل الممارسات التشريعية في العالم مع مراعاة الاتفاقيات والتشريعات الدولية والإقليمية.
- ضمان أن تكون الإصلاحات التشريعية المراد إدخالها متوازنة بين التصدي للمخاطر و الجرائم السيبرانية وحماية الحقوق و الحريات و خاصة الخصوصية وحرية التعبير عبر الإنترنات.
- إحداث وحدات متخصصة لدى أعوان الضابطة العدلية للتحقيق في الجرائم السيبرانية.
- تشجيع الضحايا على التبليغ عن الجرائم السيبرانية لتجميع المعلومات وإتاحة التبليغ عن بعد.
- بناء القدرات في صياغة القوانين والأنظمة المتعلقة بالأمن السيبراني.
- القيام بحملات توعوية و تكوينية للمتدخلين في التصدي للجرائم السيبرانية من قضاة وأعوان الضابطة العدلية و المشرعين والمحامين و عدول التنفيذ.
- القيام بحملات توعوية لفائدة المواطنين و خاصة بعض الفئات المستهدفة بالجرائم السيبرانية أو الفئات الهشة مثل الأطفال و نشر ثقافة الخصوصية و الأمن السيبراني.
- العمل على تطوير الإطار القانوني الذي تمارس فيه فرق التصدي و الإستجابة لطوارئ الحاسوب و تطوير المبادرات في مجال " القرصنة الأخلاقية" و تذليل الصعوبات التي تعيقها.
- تطوير أطر و أساليب و إجراءات التعاون القضائي بين الدول العربية و غيرها من الدول قصد تجنب الملاذات الآمنة لأرتكاب الجرائم السيبرانية.
- العمل على تسخير مهارات " القرصنة الأخلاقية " وتطويرها من خلال عقد مسابقات المواهب و"الهاكاتون" و وضع أدلة لمجموعات الباحثين المحليين المشتغلين في مجال القرصنة الأخلاقية
- تعزيز الشراكات بين القطاع العام والقطاع الخاص حسب نهج تعاوني وتآزري.
- العمل على دعم أطر التعاون العربي على مستوى التصدي للمخاطر و الجرائم السيبرانية حسب نهج تعاوني وتآزري.
- تشجيع الإدارات العامة و المؤسسات الخاصة و الجمعيات على وضع مدونات السلوك المتعلقة بالأمن السيبراني و بحماية الخصوصية.

قوانين ولوائح الأمن السيبرني

- التطرق إلى جميع أنواع الجرائم الإلكترونية
- حماية التقنيات الحالية والناشئة
- تعزيز حماية الشركات الصغيرة والمتوسطة

بيئة متكاملة وحيوية للأمن السيبرني

- دعم الشركات الناشئة وتعزيز البحث والتطوير في مجال الأمن السيبرني
- تطوير القدرات في الأمن السيبرني
- تعزيز وعي الأفراد بالمخاطر السيبرنية وبأهمية الأمن السيبرني
- تشجيع التميز في الأمن السيبراني

الخطة الوطنية للاستجابة للحوادث السيبرنية

- وسيلة موحدة للإبلاغ عن الحوادث السيبرنية
- نموذج موحد لتقييم الخطورة وخطة للتعامل مع الحوادث السيبرنية
- مشاركة المعلومات الاستخبارية بين الجهات

برنامج حماية البنية التحتية للمعلومات الحيوية

- تحديد الأصول الحيوية
- وضع معايير عالمية لإدارة المخاطر
- عمليات فعالة للإبلاغ والامتثال والاستجابة

الشراكات

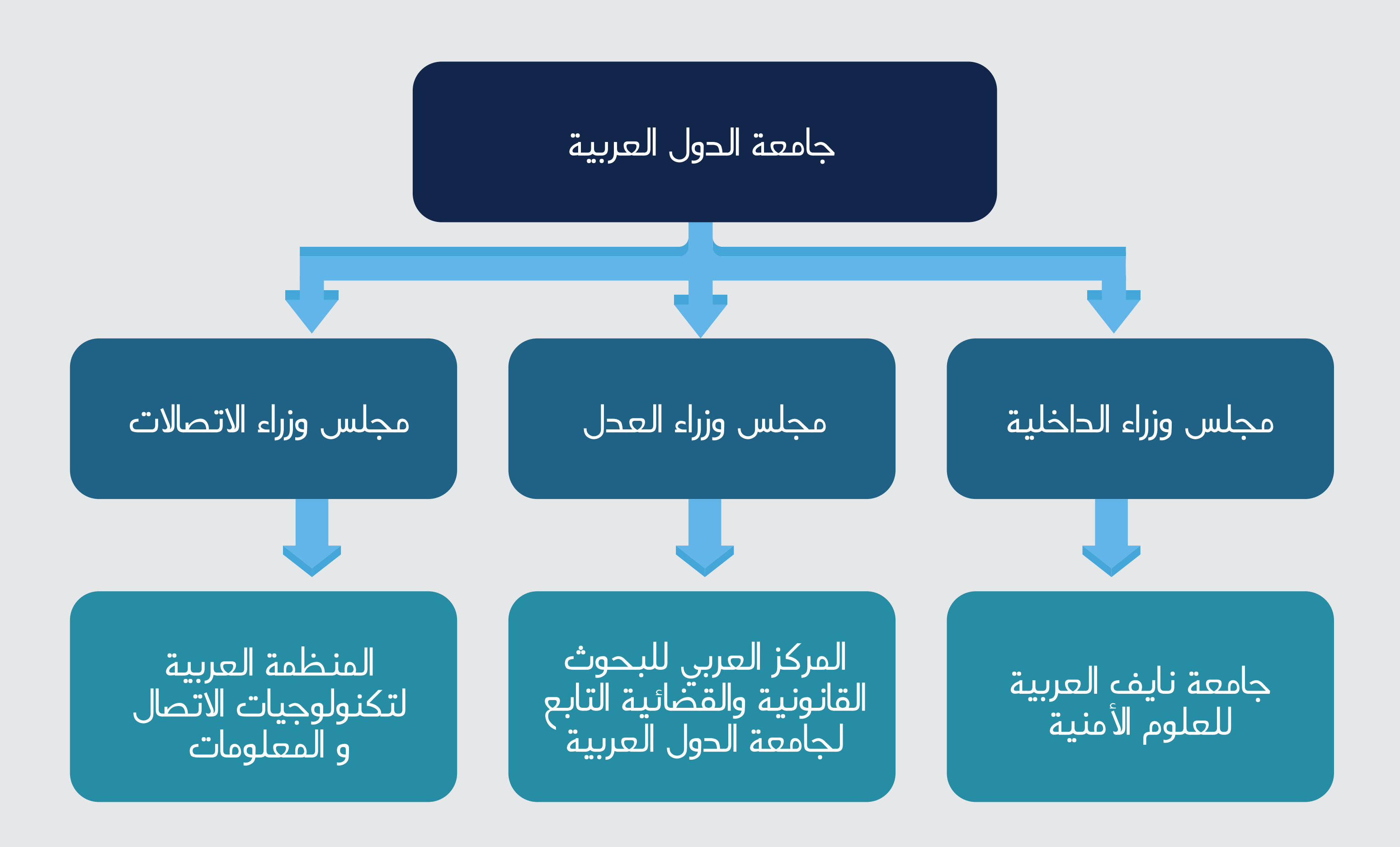
- القطاع الحكومي
- القطاع الخاص
- المؤسسات الأكاديمية
- الجمعيات والمنظمات الاقليمية والدولية

5.2 عناصر الخطة العملية

تعتمد الخطة العملية على العناصر الأساسية التالية

5.2.1.1 حوكمة الأمن السيبراني في المنطقة العربية

بالنظر الى هيكلية العمل العربي المشترك في اطار جامعة الدول العربية و باعتبار اختصاصات كل هيئة و منظمة، فاننا نقترح إنشاء مجلس إقليمي أو أي إطار اقليميى يقوم بإدارة و اقتراح و انشاء المبادرات الإقليمية و متابعة تنفيذها خاصة في مجالات تنمية القدرات في مجال الأمن السيبراني وتطوير البحث العلمي وملاءمة التشريعات المتعلقة بالسلامة المعلوماتية والجريمة السيبرانية. كما يقوم بوضع و متابعة تطور المؤشرات الإقليمية و نشرها و أيضا بتنسيق الاستعدادات لمجابهة الجرائم و المخاطر السيبرانية التي تتزايد يوما بعد يوم.



المبادرات الاقليمية

و من المبادرات الإقليمية التي نقترحها

التوجه الى الانشاء الرسمي لتجمع عربي معترف به اقليميا و دوليا و يكون تحت مسمى " عرب سرت" (Arab CERT) ، و يمكن انشاء هذا التجمع بشكل افتراضي كمرحلة أولى ليكون أحد أهم خطوات دعم التعاون العربي في هذا المجال الحيوي و الاستراتيجي. سيكون من مهام هذا التجمع:

- تنسيق مركز اتصال و تواصل اقليمي دولي لرصد الحوادث الأمنية التي تتعلق بتكنولوجيا المعلومات والاتصالات
- تقديم المعلومات الدقيقة والآنية عن التهديدات الأمنية ونقاط الضعف الحالية أو الناشئة و الحلول التقنية المقترحة
- رصد و توفير التدابير الإستباقية لتقليل الحوادث الأمنية
- التنسيق مع مراكز الاستجابة لطوارئ الحاسوب الوطنية و على الأصعدة الإقليمية والدولية

اعداد و تطوير و تحيين ملائمة التشريعات و القوانين المرجعية خاصة في ظل التطور السريع للتوجهات التكنولوجية

بالاعتماد على دراسات مقاربة تخص هذه القوانين:

- قوانين الامن السيبراني
- مجابهة الجريمة الاكترونية
- حماية البيانات و المعطيات الشخصية
- المعاملات الإلكترونية
- حماية الأطفال والشباب في الفضاء الرقمي

تنمية القدرات في مجال تكنولوجيات المعلومات والاتصال وتطوير البحث العلمي و ذلك

- بتطوير منهج تدريبي خاص معتمد ينهي الى شهادة مهنية خبير عربي في الأمن السيبراني ويقع تنفيذه من طرف شبكة من المعاهد العليا والجامعات والمؤسسات التعليمية العربية معتمدة.
- بوضع حزمة من المبادرات الإقليمية المحفزة في مجال البحث العلمي و الابتكار في مجال الامن السيبراني و حماية الشبكات و بانشاء المسابقات العربية المتخصصة في مجال الEthical hacking
- انشاء قاعدة بيانات للخبراء العرب في ميدان الأمن السيبراني

إنشاء مرصد لمؤشرات الأمن السيبراني في المنطقة العربية

و ذلك

- بتطوير منصة يقع تحيينها بصفة دورية تقوم برصد و عرض كل المؤشرات المتعلقة بالأمن السيبراني في المنطقة العربية .كما تقوم المنصة بتقاسم كل الوثائق المرجعية العامة للمتعلقة بالخطط الاستراتيجية و الوطنية
- صياغة معايير إقليمية تراعي أفضل الممارسات العالمية مع الأخذ في الاعتبار الحاجيات الخاصة للدول العربية

6. خاتمة

نحن على إقتناع تام أنه فيما يعلّق بالأمن السيبراني، تبذل العديد من الدول الدول العربية جهودا كبيرة، ولكن الطريق لا تزال طويلة للتعامل مع المخاطر السيبرانية التي تتزايد يوما بعد يوم، وهو ما يتطلّب توحيد الجهود على المستوى العربي والإقليمي والدولي لإيجاد حلول شاملة ومستدامة.

اليوم، أكثر من أي وقت مضى، نحتاج إلى تسريع خطواتنا نحو علاقات تعاون قوية من أجل إنشاء نهج تعاوني لتعزيز فضاء رقمي مفتوح وحر وآمن للجميع في كل مكان.

وتصبو المنظمة العربية لتكنولوجيات الاتصال والمعلومات أن تكون هذه المبادرة حلقة الوصل بين الدول العربية في مجال السلامة المعلوماتية والأمن السيبراني. ونتطلع إلى التعاون مع كل الدول العربية والجهات الفاعلة في المجال من أجل تحقيق أهدافنا المشتركة في المجال.



7. الملاحق

وضع رؤية عربية مشتركة
في مجال التكنولوجيا والاقتصاد الرقمي والأمن السيبراني

إن مؤتمر القمة العربية التنموية: الاقتصادية والاجتماعية في دورته العادية الرابعة،

- **بعد اطلاعه على:**
  - مذكرة الأمانة العامة،
  - قرار المجلس الاقتصادي والاجتماعي رقم (2209) د.غ.ع بتاريخ 2018/12/20،
  - نتائج أعمال الاجتماع المشترك للمندوبين الدائمين وكبار المسؤولين والاجتماع المشترك لوزراء الخارجية والوزراء المعنيين بالمجلس الاقتصادي والاجتماعي للتحضير للقمة،
- **وبعد الاستماع إلى إيضاحات الأمانة العامة،**
- **وفي ضوء المناقشات،**

يُقــرّر

1. تثمين مبادرة حضرة صاحب السمو أمير دولة الكويت الشيخ صباح الأحمد الجابر الصباح لإنشاء صندوق للإستثمار في مجالات التكنولوجيا والاقتصاد الرقمي برأس مال وقدره مائتي مليون دولار أمريكي بمشاركة القطاع الخاص، ومساهمة دولة الكويت بمبلغ 50 مليون دولار، وكذلك مساهمة دولة قطر بمبلغ 50 مليون دولار من رأس مال هذا الصندوق بما يعادل نصف حجمه، على أن يوكل إلى الصندوق العربي للإنماء الاقتصادي والاجتماعي مسؤولية إدارة هذه المبادرة التنموية.
2. دعوة الدول العربية إلى دعم هذه المبادرة للإسهام في تعزيز الاقتصاد العربي المشترك وخلق فرص عمل واعدة للشباب العربي، وحث البنوك ومؤسسات التمويل العربية المشتركة المساهمة في دعم هذه المبادرة بالطرق التي توفر لها الاستمرارية لتحقيق أهدافها المنشودة.
3. تكليف الأمانة العامة بالتنسيق مع المجالس الوزارية المختصة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والخبرات المتوفرة لدى الدول العربية، بدراسة وضع رؤية عربية مشتركة في مجال التكنولوجيا والاقتصاد الرقمي والأمن السيبراني.

(ق. ق: 56 د.ع (4) – ج 3 – 2019/1/20)



الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجـة :

إن الدول العربية الموقعة،

رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

والتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

فقد اتفقت على ما يلي :

الفصل الأول
أحكام عامة

المادة الأولى : الهدف من الاتفاقية :

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادة الثانية : المصطلحات :

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1- **تقنية المعلومات** : أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة.

2- **مزود الخدمـة** : أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3- **البيـانـات** : كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها ...



4- **البرنامج المعلوماتي**: مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.

5- **النظام المعلوماتي**: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

6- **الشبكة المعلوماتية**: ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

7- **الموقـــع** : مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

8- **الالتقــاط** : مشاهدة البيانات أو المعلومات أو الحصول عليها.

9- **معلومات المشترك**: أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ - نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.

ب- هويــة المشــترك وعنوانــه البريــدي أو الجغرافــي أو هاتفــه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.

ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادة الثالثة: **مجالات تطبيق الاتفاقية**:

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

1 - ارتكبت في أكثر من دولة.

2- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.

3- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.

4- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

المادة الرابعة: **صون السيادة**:

1- تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الثاني

التجريم

المادة الخامسة: **التجريم**:

تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية.



المادة السادسة : جريمة الدخول غير المشروع :

1- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ب- الحصول على معلومات حكومية سرية.

المادة السابعة : جريمة الاعتراض غير المشروع :

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادة الثامنة : الاعتداء على سلامة البيانات :

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.

2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم.

المادة التاسعة : جريمة إساءة استخدام وسائل تقنية المعلومات :

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب- كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

المادة العاشرة : جريمة التزوير :

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادة الحادية عشرة : جريمة الاحتيال :

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.



3- تعطيل الأجهزة والبرامج والمواقع الالكترونية.

المادة الثانية عشرة : جريمة الإباحية :

1- انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.
3- يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

المادة الثالثة عشرة : الجرائم الأخرى المرتبطة بالإباحية :

المقامرة والاستغلال الجنسي.

المادة الرابعة عشرة : جريمة الاعتداء على حرمة الحياة الخاصة :

الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات .

المادة الخامسة عشرة : الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات :

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المادة السادسة عشرة : الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات :

1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.
2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.
3- الاتجار بالأشخاص.
4- الاتجار بالأعضاء البشرية.
5- الاتجار غير المشروع بالأسلحة.

المادة السابعة عشرة : الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة :

انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

المادة الثامنة عشرة : الاستخدام غير المشروع لأدوات الدفع الالكترونية :

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.



2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.
3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة التاسعة عشرة: الشروع والاشتراك في ارتكاب الجرائم:

1- الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.
2- الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.
3- يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً.

المادة العشرون: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية:

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً.

المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

الفصل الثالث

الأحكام الإجرائية

المادة الثانية والعشرون: نطاق تطبيق الأحكام الإجرائية:

1- تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والاجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.
2- مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على:
   أ- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية.
   ب- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات.
   ج- جمع الأدلة عن الجرائم بشكل إلكتروني.
3- أ- يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا



يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة الثلاثين، وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادة التاسعة والعشرين.

ب- كما يجوز للدولة الطرف أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي تبث بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية:

- يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين.
- لا تستخدم شبكات اتصال عامة وليست مرتبطةً بتقنية معلومات أخرى سواء كانت عامة أو خاصة.

وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين التاسعة والعشرين والثلاثين.

المادة الثالثة والعشرون : التحفظ العاجل على البيانات المخزنة في تقنية المعلومات :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوماً قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للابقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.

المادة الرابعة والعشرون : التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين :

تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل :

1 - ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

2- ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

المادة الخامسة والعشرون : أمر تسليم المعلومات :

تلتزم كل دولة طرف بتبني الاجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى :



1 - أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.
2 - أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمه أو تحت سيطرته.

المادة السادسة والعشرون : تفتيش المعلومات المخزنة :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى :
أ - تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.
ب - بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.
2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1 - أ) اذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

المادة السابعة والعشرون : ضبط المعلومات المخزنة :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقره (1) من المادة السادسة والعشرين من هذه الاتفاقية .
هذه الإجراءات تشمل صلاحيات :
أ - ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات .
ب - عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها .
ج - الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.
د - إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها .
3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (2,1) من المادة السادسة والعشرين من هذه الاتفاقية.

المادة الثامنة والعشرون : الجمع الفوري لمعلومات تتبع المستخدمين :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من :
أ - جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.
ب - إلزام مزود الخدمة ضمن اختصاصة الفني بأن :



- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،أو
- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقره (1 - أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3 - تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

المادة التاسعة والعشرون : **إعتراض معلومات المحتوى** :

1 - تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من :
أ - الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو
ب - التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية معلومات .

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1 - أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

الفصل الرابع
التعاون القانوني والقضائي

المادة الثلاثون : **الاختصاص** :

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت :
أ - في إقليم الدولة الطرف.
ب- على متن سفينة تحمل علم الدولة الطرف.
ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.



د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم.

المادة الحادية والثلاثون: تسليم المجرمين:

1- أ- هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الاطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب- إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق.

2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبرجرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3- إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة.

4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول.

5- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.

6- يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.

7- أ- تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في



ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

ب- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائماً.

المادة الثانية والثلاثون : المساعدة المتبادلة :

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين.

3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك إستخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات.

4- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية.

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف.

المادة الثالثة والثلاثون : المعلومات العرضية المتلقاة :

1- يجوز لأي دولة طرف - ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف.

2- قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات, وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات، وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.



المادة الرابعة والثلاثون : الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة :

1- تطبق بنود الفقرات (2-9) من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة والمطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار اليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي.

2- أ- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.

ب- على السلطات المركزية أن تتصل ببعضها مباشرة.

ج- على كل دولة طرف - وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة.

د- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائماً.

3- يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة.

4- يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها.

5- قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذا سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية.

6- تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب, وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.

7- يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر الكافي لتنفيذ الطلب, وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.

8- أ- في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.

ب- يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول.

ج- حيثما يتم تقديم طلب حسب الفقرة(أ) ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك.



د. إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

هـ. يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الإنضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.

المادة الخامسة والثلاثون : رفض المساعدة :

يجوز للدولة الطرف المطلوب منها المساعدة - بالاضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثين الفقرة (4) أن ترفض المساعدة إذا:

1- كان الطلب متعلقاً بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية.

2- اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادته أو أمنه أو نظامه أو مصالحه الأساسية.

المادة السادسة والثلاثون : السرية وحدود الاستخدام :

1- عندما لايكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع الساري بين الدول الأطراف الطالبة والمطلوب منها فيجب تطبيق بنود هذه المادة ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق أي من فقرات هذه المادة أو كلها.

2- يجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب بشرط:

أ - الحفاظ على عنصر السرية للدولة الطرف الطالبة للمساعدة ولا يتم الالتزام بالطلب في غياب هذا العنصر.

ب- عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب.

3- إذا لم تستطع الدولة الطرف الطالبة الالتزام بالشرط الوارد في الفقرة (2) فيجب عليها إعلام الدولة الطرف الأخرى والتي ستقرر بعدها مدى إمكانية توفير المعلومات، وإذا قبلت الدولة الطرف الطالبة بهذا الشرط فهو ملزم لها.

4- أي دولة طرف توفر المعلومات أو المواد بحسب الشرط في الفقرة (2) لتوفير المعلومات يجوز لها أن تطلب من الدولة الطرف الأخرى أن تبرر استخدام المعلومات أو المواد.

المادة السابعة والثلاثون. الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات :

1- لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

2- يجب أن يحدد طلب الحفظ حسب الفقرة (1) ما يلي:

أ- السلطة التي تطلب الحفظ.

ب- الجريمة موضوع التحقيق وملخصاً للوقائع.

ج- معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة.



د- أيـة معلومـات متـوفرة لتحديـد المسـؤول عـن المعلومـات المخزنـة أو موقـع تقنيـة المعلومات.

هـ- موجبات طلب الحفظ.

و- رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصـول أو الضبط أو تأمين أو كشف معلومات تقنية المعلومات المخزنة.

3- عند استلام إحدى الدول الأطراف الطلب من دولة طرف أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب فلا يشترط وجود إزدواجية التجريم للقيام بالحفظ.

4- أي دولة طرف تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الاتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب للاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

5- بالاضافة لذلك، يمكن رفض طلب الحفظ إذا :

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- إعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

6- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب.

7- أي حفظ ناجم عن الاستجابة للطلب المذكور في الفقرة (1) يجب أن يكون لفترة لا تقل عن (60) يوماً من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات. وبعد إستلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب.

المادة الثامنة والثلاثون : الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة :

1- حيثما تكتشف الدولة الطرف المطلوب منها - في سياق تنفيذ الطلب حسب المادة السابعة والثلاثين لحفظ معلومات تتبع المستخدمين الخاصة باتصالات معينة - بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات.

2- يمكن تعليق كشف معلومات تتبع المستخدمين حسب الفقره (1) إذا:

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- اعتبرت الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سلامتها أو أمنها أو نظامها أو مصالحها.



المادة التاسعة والثلاثون : التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة :

1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.

2- تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.

3- تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضه للفقدان أو التعديل.

المادة الأربعون : الوصول إلى معلومات تقنية المعلومات عبر الحدود :

يجوز لأي دولة طر، وبدون الحصول على تفويض من دولة طرف أخرى:

1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات .

2- أن تصل أو تستقبل - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

المادة الحادية والأربعون : التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين :

1- على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينه في أقاليمها والتي تبث بواسطة تقنية المعلومات.

2- على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية.

المادة الثانية والأربعون : التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى :

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينه تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية .

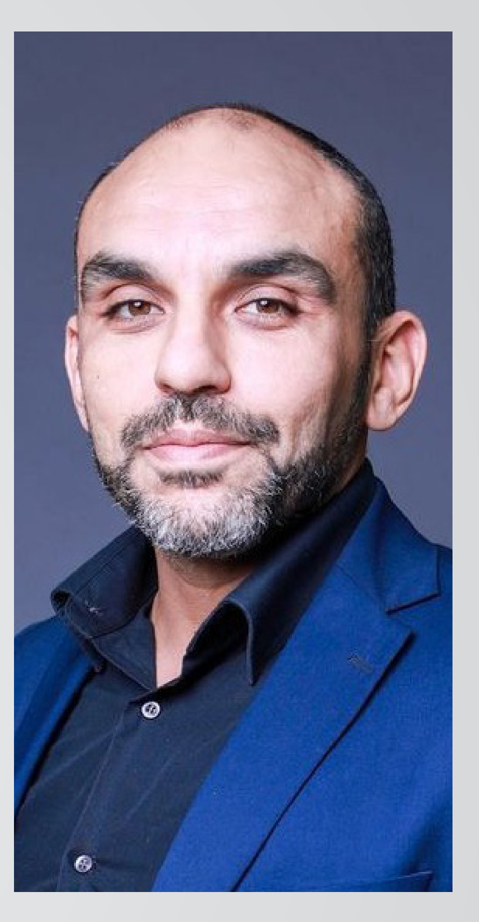
المادة الثالثة والأربعون : جهاز متخصص :

1- تكفل كل دولة طرف، وفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات

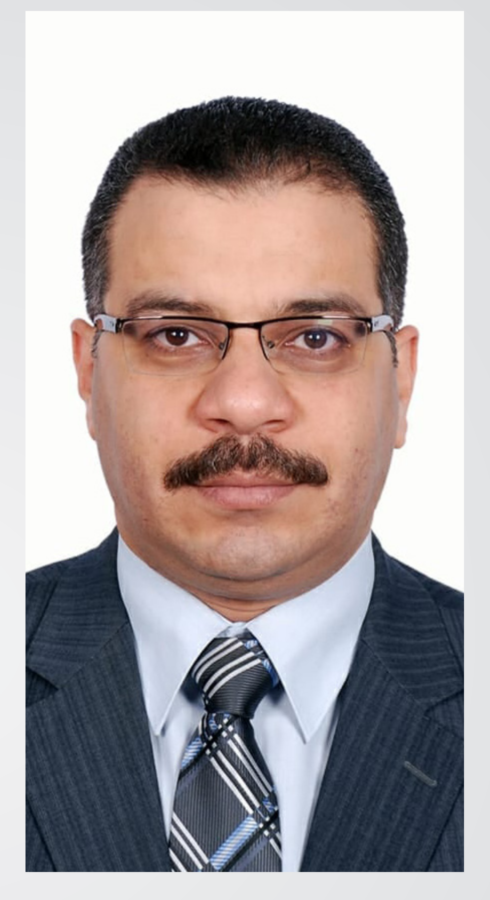
فريق إعداد الملف



د. كمال الرزقي



د. محمد حمدي



د. عادل عبد المنعم

فريق التنسيق و المراجعة :

المهندس سامي تريمش

السيدة ندى العبيدي




AICTO
ARAB INFORMATION AND COMMUNICATION TECHNOLOGY ORGANIZATION



المنظمة العربيـة لتكنولوجيـات الاتصـال والمعلومات، هي منظمة حكومية عربيـة تعمـل تحـت رايـة جامعـة الـدول العربيـة. وتهـدف إلـى المساهمة في تطوير تكنولوجيـات المعلومـات والاتصـال في البلـدان العربيـة وتوفير الآليات الضروريـة لدعـم التعـاون والتكامـل في المجال بين أعضاء المنظمة وتطويـر سياسـات واسـتراتيجيات مشـتركة لنشـر النفـاذ العـادل المسـتدام إلـى التكنولوجيـا وتطويعهـا لخدمـة أهـداف التنميـة الاقتصاديـة وتحقيـق الرقي الاجتماعي في المنطقـة العربيـة.

-——————————————————————

العنوان : 12 نهج أنقلترا – 1000 تونس – الجمهورية التونسية
الهاتف : 0021671320713 – الفاكس : 0021671320719
البريد الالكتروني : contact@aicto.org

تونس 2021/10/21